CHAPTER 7

INSTRUMENTATION AND CONTROLS

7.1 Introduction

The instrumentation and control systems presented in this chapter provide protection against unsafe reactor operation during steady-state and transient power operations. They initiate selected protective functions to mitigate the consequences of design basis events. This chapter relates the functional performance requirements, design bases, system descriptions, and safety evaluations for those systems. The safety evaluations show that the systems can be designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power.

This chapter also discusses the instrumentation portions of the safety-related systems which function to achieve the system responses assumed in the accident analysis, and those needed to shutdown the plant. Section 7.1 describes the AP600 instrumentation and control architecture, with specific emphasis on the protection and safety monitoring system. The plant control system is also discussed briefly. Other systems are discussed in more detail in relevant sections or chapters. Section 7.2 discusses the reactor trip function, and Section 7.3 addresses the engineered safety features. Systems required for safe shutdown are discussed in Section 7.4 in support of other chapters. Safety-related display instrumentation is discussed in Section 7.5 and interlocks important to safety are presented in Section 7.6. Control systems and the diverse actuation system are discussed in Section 7.7.

Definitions

Terminology used in this chapter reflects an interdisciplinary approach to safety-related systems similar to that proposed in IEEE 603 (Reference 1).

Safety System - The aggregate of electrical and mechanical equipment necessary to mitigate the consequences of design basis events. The safety system for the AP600 is composed of the protection and safety monitoring system equipment, safety-related display instrumentation, and essential auxiliary supporting systems.

Protection and Safety Monitoring System - The aggregate of electrical and mechanical equipment which senses generating station conditions and generates the signals to actuate reactor trip and engineered safety features, and which provides the equipment necessary to monitor plant safety-related functions during and following designated events.

Protective Function - Any one of the functions necessary to mitigate the consequences of a design basis event. Protective functions are initiated by the integrated protection cabinets and will be accomplished by the trip and actuation subsystems. Examples of protective functions are reactor trip and engineered safety features (such as valve alignment and containment isolation).

Actuated Equipment - The assembly of prime movers and driven equipment used to accomplish a protective function (such as solenoids, shutdown rods, and valves).

Actuation Device - A component that directly controls the motive power for actuated equipment (such as circuit breakers, relays, and pilot valves).

Division - One of the four redundant segments of the safety system. A division includes its associated sensors, field wiring, cabinets, and electronics used to generate one of the redundant actuation signals for a protective function. It also includes the power source and actuation signals.

Channel - One of the several separate and redundant measurements of a single variable used by the protection and safety monitoring system in generating the signal to initiate a protective function. A channel can lose its identity when it is combined with other inputs in a division.

Degree of Redundancy - The number of redundant channels monitoring a single variable, or the number of redundant divisions which can initiate a given protective function or accomplish a given protective function. Redundancy is used to maintain protection capability when the safety-related system is degraded by a single random failure.

System-Level Actuation - Actuation of a sufficient number of actuation devices to effect a protective function.

Component-Level Actuation - Actuation of a single actuation device (component).

7.1.1 The AP600 Instrumentation and Control Architecture

Figure 7.1-1 illustrates the instrumentation and control architecture for the AP600. The figure shows two major sections separated by the monitor bus.

The lower portion of the figure includes the plant protection, control, and monitoring functions. At the left are the protection and safety monitoring system cabinets. They include the reactor trip subsystem and the engineered safety features actuation subsystem. These cabinets, their related sensors, and the reactor trip switchgear are four-way redundant. This redundancy permits the use of automatically invoked bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic.

The engineered safety features actuation cabinets perform system-level logic calculations, such as initiation of the passive residual heat removal system. They receive inputs from the integrated protection cabinets and the main control room.

The protection logic cabinets provide the capability for on-off control of individual safety-related plant loads. They receive inputs from the engineered safety features actuation cabinets, remote shutdown workstation and the main control room.

The control cabinets perform nonsafety-related instrumentation and control functions using both discrete (on/off) and modulating (analog) type actuation devices.

The nonsafety-related monitor bus, which horizontally divides the figure, is a high speed, redundant communications network that links systems of importance to the operator. Safety-related systems are connected to the monitor bus through qualified isolation devices so that their functions are not compromised by failures elsewhere.

Plant protection, control, and monitoring systems feed real-time data into the bus for use by the control room and the computer system.

The upper portion of the figure depicts the control rooms and distributed computer system. The main control room is implemented as a set of compact operator consoles featuring color graphic displays and soft control input devices. The graphics are supported by a set of microprocessor-based graphics workstations that take their input from the monitor bus. An advanced alarm system, implemented in a similar technology, is also provided.

The computer system is implemented in a distributed architecture. The working elements of the distributed computer system are graphics workstations, although their graphics capability is secondary to their computing performance. The distributed computer system obtains its input from the monitor bus and delivers its output over the bus to other users.

There is another grouping of the systems shown on this figure. They are the seven sets of systems enclosed by the dotted line boxes. These are groups of systems that share similar characteristics, making it convenient to treat them together in this document. These systems are the following:

- Protection and safety monitoring system
- Special monitoring system
- Plant control system
- Operation and control centers system
- Diverse actuation system
- Data display and processing system
- Incore instrumentation system

WCAP-13633 (Reference 12) describes the diversity and defense-in-depth features of the AP600 instrumentation and control architecture.

Protection and Safety Monitoring System

The protection and safety monitoring system provides the safety-related functions necessary to control the plant during normal operation, to shutdown the plant, and to maintain the plant in a safe shutdown condition. The protection and safety monitoring system controls safety-related components in the plant that are operated from the main control room or remote shutdown workstation.

In addition, the protection and safety monitoring system provides the equipment necessary to monitor the plant safety-related functions during and following an accident as required by Regulatory Guide 1.97.

The protection and safety monitoring system includes the following:

- Integrated protection cabinets
- Engineered safety features actuation cabinets
- Protection logic cabinets
- Qualified data processing cabinets
- Qualified data processing I/O cabinets
- Qualified displays
- Reactor trip switchgear
- Sensors
- Main control room and remote shutdown workstation multiplexers
- Main control room/remote shutdown workstation transfer panels

Special Monitoring System

The special monitoring system does not perform any safety-related or defense-in-depth functions. The special monitoring system consists of specialized subsystems that interface with the instrumentation and control architecture to provide diagnostic and long-term monitoring functions.

The special monitoring system includes the metal impact monitoring system. The metal impact monitoring system detects the presence of metallic debris in the reactor coolant system when the debris impacts against the internal parts of the reactor coolant system. The metal impact monitoring system includes digital circuit boards, controls, indicators, power supplies and remotely located sensors and related signal processing devices. The sensors and their related signal processing devices are mounted in pairs to maintain the impact monitoring function if a sensor fails in service. The metal impact monitoring system is described in subsection 4.4.6.4.

Plant Control System

The plant control system provides the functions necessary for normal operation of the plant from cold shutdown through full power. The plant control system controls nonsafety-related components in the plant that are operated from the main control room or remote shutdown workstation.

The plant control system contains nonsafety-related control and instrumentation equipment to change reactor power, control pressurizer pressure and level, control feedwater flow, and perform other plant functions associated with power generation.

The plant control system includes the following:

- Distributed controllers
- Signal selectors
- Rod control cabinets
- Rod drive motor-generator sets
- Pressurizer heater control interface
- Rod position indication cabinets
- Process bus multiplexers
- Controls and indication
- Process bus
- Sensors

Diverse Actuation System

The diverse actuation system is a nonsafety-related, diverse system that provides an alternate means of initiating reactor trip and selected engineered safety features, and providing plant information to the operator. The diverse actuation system is described in subsection 7.7.1.11.

Operation and Control Centers System

The operation and control centers system includes the main control room, the technical support center, the remote shutdown room, emergency operations facility, local control stations and associated workstations for each of these centers. With the exception of the control console structures, the equipment in the control room is part of the other systems (for example, protection and safety monitoring system, plant control system, data display and processing system).

The boundaries of the operation and control centers system for the main control room and the remote shutdown workstation are the signal interfaces with the plant components. These interfaces are via the plant protection and safety monitoring system processor and logic circuits, which interface with the reactor trip and engineered safety features plant components; the plant control system processor and logic circuits, which interface with the nonsafety-related plant components; and the plant monitor bus, which provides plant parameters, plant component status, and alarms.

Data Display and Processing System

The data display and processing system provides the equipment used for processing data that will result in nonsafety-related alarms and displays for both normal and emergency plant operations, generating these displays and alarms, providing analysis of plant data, providing plant data logging and historical storage and retrieval, and providing operational support for plant personnel.

The data display and processing system also contains the monitor bus, which is a redundant data highway that links the elements of the AP600 instrumentation and control architecture.

Incore Instrumentation System

The primary function of the incore instrumentation system is to provide a three-dimensional flux map of the reactor core. This map is used to calibrate neutron detectors used by the protection and safety monitoring system, as well as to optimize core performance. A secondary function of the incore instrumentation system is to provide the protection and safety monitoring system with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The incore instrument assemblies house both fixed incore detectors and core exit thermocouples. The incore instrumentation system is described in subsection 4.4.6.1.

7.1.2 General Protection Subsystem Configuration

The protection and safety monitoring system is illustrated in Figure 7.1-2. The functions of the protection and safety monitoring system have been decomposed into physically and electrically separate microprocessor based subsystems. Each subsystem is located on an independent computer bus to prevent propagation of failures and to enhance availability. In most cases, each subsystem is implemented in a separate card chassis. Subsystem independence is maintained through the use of the following:

- Separate dc power sources with output protection to prevent interaction between subsystems upon failure of a subsystem.
- Separate input or output circuitry to maintain independence at the subsystem interfaces.
- Deadman signals: A device, circuit, or function that forces a predefined operating condition upon the cessation of a normally dynamic input parameter to improve the reliability of hard-wired data that crosses the subsystem interface.
- Optical coupling or resistor buffering between two subsystems or between a subsystem and an input/output (I/O) module.

WCAP-13382 (Reference 3) provides a description of the hardware elements which comprise the protection and safety monitoring system configuration. WCAP-14080 (Reference 8) provides a description of the software architecture and operation.

7.1.2.1 Functional Components

The type and number of boards used to implement the functions of a microprocessor based subsystem are purposely limited to aid serviceability and to restrict the number of spares. In addition, the basic function of a particular board remains fixed among subsystems to facilitate the development and maintenance of the subsystem software. IEEE 796 (Reference 2) bus cards are typically used to provide functions as listed below.

Functional Processor

The functional processor performs the major computations required to achieve the specific function of the microprocessor based subsystem. Tasks performed by the functional processor include movement of data between subsystem memories or I/O registers for the purpose of input or output, on-line compensation of the analog inputs, conversion of input data to engineering units, and diagnostic testing. A functional processor is included in each subsystem.

Bus Monitor Card

The bus monitor performs a diagnostic reset function upon failure of the functional processor or the IEEE 796 bus, as determined by the lack of a deadman signal. If the functional processor's deadman signal stops and the diagnostic reset is enabled, the bus monitor card resets the functional processor. The card also monitors the local temperature, dc voltages, and cabinet door closure. It provides this data to the functional processor for evaluation.

Data Link Processor

Serial communications required by the subsystem, with the exception of the maintenance ports, are performed by this board. Onboard status and diagnostic checking features are also provided.

Data Highway Control

The highway control processor provides the interface between the engineered safety features actuation cabinets and the logic bus of the protection logic. Onboard status and diagnostic checking is performed. This card is found in the microprocessor based subsystems of the engineered safety features actuation cabinets.

Parallel I/O Card

The handling of discrete I/O signals in the subsystem is accomplished by this card. Subsystem to I/O module and subsystem to test/maintenance panel interfaces use this card.

Isolated Parallel I/O Card

In the few instances where subsystem to subsystem I/O is required, optically coupled I/O is used. The operation of the card is the same as the parallel I/O card with the addition of optical isolation.

Analog Input Processor

The input processing of analog input signals is accomplished by this card. The analog inputs are read and digital signal conditioning (such as averaging, and filtering algorithms) is performed on the data. Analog to digital conversion, signal status checks, input calibration

readings, and onboard diagnostics are also performed. Filtered input data is provided to the functional processor for calibration calculations.

Universal Site Memory Expansion Card

A general purpose memory board is used in instances where the functional processor does not possess sufficient memory to perform its required functions.

Digital/Analog Conversion Card

Analog outputs are used to generate test inputs to the protection and safety monitoring system's analog I/O boards. The digital values are generated by the functional processor in the automatic tester subsystem and placed in registers on the digital/analog board. The analog values are then output onto the analog test bus.

Test Bus Controller

A communication bus is used to control the components located on both the analog and digital test buses. This card is found in the automatic tester subsystems.

7.1.2.2 Integrated Protection Cabinet Subsystems

The integrated protection cabinet contains the necessary equipment to perform the following functions:

- Permit acquisition and analysis of the sensor inputs required for reactor trip and engineered safety features actuation calculations.
- Perform computation or logic operation on variables based on these inputs.
- Provide trip signals to the reactor trip switchgear and engineered safeguards actuation data to the engineered safety features actuation cabinets, as required.
- Permit manual trip or bypass of each individual automatic reactor trip function and permit manual actuation or bypass of each individual automatic engineered safety features actuation function.
- Provide data to external systems.
- Provide functional diversity for the reactor trips and engineered safety features actuations.
- Provide separate input circuitry for control functions requiring input from sensors which are also required for protection functions.

To conform with the system criteria concerning separation and diversity, the functions of the protection and safety monitoring system are implemented in 10 microprocessor based subsystems. These subsystems are the following:

- Reactor trip group 1
- Reactor trip group 2
- Global trip
- Trip enable
- Engineered safety features group 1
- Engineered safety features group 2
- Communication
- Automatic tester
- Nuclear instrumentation signal and processing and control (NISPAC) 1
- Nuclear instrumentation signal and processing and control (NISPAC) 2

Figure 7.1-3 illustrates the integrated protection cabinet.

7.1.2.2.1 Reactor Trip Subsystems

The reactor trip functions are divided into two functionally diverse subsystems for accident protection. Independence of the functionally diverse trips is maintained in the reactor trip groups from the input circuitry through to the dynamic trip bus. The primary function of the reactor trip subsystems is to process input data and provide a partial trip signal to the dynamic trip bus whenever the preset limit of each protection function is exceeded. The following trip functions are implemented in the reactor trip subsystems:

- Reactor Trip Group 1 Subsystem
  - High source range neutron flux
  - Low reactor coolant pump speed
  - Low reactor coolant flow
  - Overtemperature ΔT
  - Overpower ΔT
  - High reactor coolant pump bearing water temperature
  - High compensated pressurizer level
- Reactor Trip Group 2 Subsystem
  - High intermediate range neutron flux
  - High power range flux low setpoint
  - High power range flux high setpoint
  - High positive rate power range neutron flux
  - Low pressurizer pressure
  - High pressurizer pressure
  - High-2 steam generator narrow range level
  - Low steam generator narrow range level

To perform the protective function calculations, the subsystems require data from field sensors. The subsystems also use manual inputs from the main control room. The results of the calculations drive the corresponding partial trip circuitry of the dynamic trip bus to the prescribed state. Deadman circuitry contained within the dynamic trip bus logic and status readback to the reactor trip subsystem, provides confidence in the activation of a partial trip. Transfer of the information between the reactor trip subsystems and the dynamic trip logic is performed by parallel I/O isolated by the dynamic trip bus.

7.1.2.2.2 Manual Controls and Indications

The two reactor trip subsystems provide partial trip signals to the dynamic trip bus via parallel I/O. The dynamic trip bus provides the ability to place each partial reactor trip signal in normal, manual trip, or manual bypass mode. The trip/normal/bypass switches allow each individual partial trip signal to be manually tripped or bypassed by plant personnel should a failure be detected in the associated input circuitry or sensor rather than bypassing an entire division. Indicators are placed adjacent to the trip/normal/bypass switch for display of the partial trip signal status. Parallel I/O transfers the partial trip signals from the reactor trip subsystems to the trip/normal/bypass switch.

7.1.2.2.3 Trip Logic Function

The trip logic function acts to initiate a reactor trip when a trip function in two-out-of-four independent safety divisions is in a partial trip state. The trip logic function also provides for the bypass of trip functions and safety divisions to accommodate tests and maintenance. The overall system logic implemented by the trip logic function is discussed in subsection 7.1.2.10.

The trip logic function is composed of three primary functions:

- The global trip subsystem provides partial trip/bypass status to the other divisions and division trip and bypass status to the other divisions; and, computes the division's global trip signal.

- The trip enable subsystem provides partial trip enable signals for each partial trip function and computes the global bypass permissive signal.

- The dynamic trip bus performs the logic to combine the partial trip and partial trip enable signals and the global trip and global bypass signals, and outputs a fail-safe trip signal to the reactor trip switchgear.

Each of the three primary functions is implemented by an independent portion of the protection and safety monitoring system. To perform the required tasks, each subsystem receives data links from the global trip subsystems in the other divisions as well as handling numerous electrically isolated parallel signals both to and from the dynamic trip bus. The integrity of the data provided to the dynamic trip bus is achieved through the use of separate "keep alive" signals provided to deadman circuitry on the dynamic logic. A detailed

discussion of the trip and bypass logic implementation is provided in WCAP-8897 (Reference 7).

7.1.2.2.3.1 Global Trip Subsystem

The global trip subsystem collects the partial trips and partial trip bypass status from the dynamic logic units of the dynamic trip bus within its own division. Sensing of the status is performed directly from the signals that are used to drive the dynamic logic. In addition, the subsystem reads the status of the reactor trip switchgear in its division. The division status information, collected by the global trip subsystem, is provided to the global trip subsystems in the other three safety divisions.

The global trip subsystem receives data from the other three divisions indicating the partial trip and partial trip bypass status of the individual trip functions. Included in the data is the division bypass status. If any of the divisions present a division bypass state, thus indicating the division is out of service either due to a global bypass or a division failure, the global trip subsystem considers each trip function within that division to be set in a partial bypass state.

Using the data received from the other three safety divisions, the global trip status of the division is computed. The global trip subsystem provides signals to the dynamic trip bus to implement a trip of the division if any of the following conditions is true for any trip function:

- Two or more partial trips exists in the other three divisions.
- Two bypasses exist in the other three divisions coincidence with the remaining division input being in a partial trip state.
- Three or more divisions are in a partial bypass state.

Each trip function is calculated separately and the states of the functions are logically treated as a logical "OR" function to produce the division trip.

When a trip of the division reactor trip switchgear occurs, the global trip subsystem records which of the trip functions produced the trip. This information is provided to the communication subsystem for output to external systems.

7.1.2.2.3.2 Trip Enable Subsystem

The trip enable subsystem receives identical partial trip and partial bypass information from the other three safety divisions similar to the global trip subsystem. Independence of the trip enable and global trip subsystems is maintained by providing separate signals to the subsystems from the signal conditioning. The partial and division trip and bypass status of the individual protection functions from the three other redundant divisions, is used to compute the trip enable and the global bypass permissive status. As in the global trip subsystem, reception of a message indicating a division bypass of any of the other divisions

or failure of the data link results in the trip enable subsystem considering each trip function within that division to be in a partial bypass state.

The trip enable subsystem provides signals to the dynamic trip bus to implement a trip of the division if any of the following conditions is true for any trip function:

- A partial trip exists in one of the other three divisions coincidence with a partial trip within the division containing the trip enable subsystem.

- Two bypasses exist in the other three divisions coincidence with a partial trip within the division containing the trip enable subsystem.

The trip enable subsystem also provides signals to the dynamic trip bus to implement a trip of the division if two divisions are bypassed. This trip signal is generated if an attempt is made to place the division, containing the trip enable subsystem, into a global bypass state after one of the three other divisions has already been placed into a similar global bypass state. This effectively alters the two-out-of-four logic, implemented by the reactor trip switchgear, to a one-out-of-two logic associated with the two divisions that remain unbypassed. If two divisions are in a global bypass state, this trip enable logic will provide a reactor trip if a bypass is attempted in a third division.

7.1.2.2.3.3 Dynamic Trip Bus

The dynamic trip bus provides a reliable means of opening the reactor trip switchgear in its own division as demanded by the individual protection functions. Signals are transferred between the dynamic trip bus and the reactor trip subsystems, global trip subsystem, trip enable subsystems, and the automatic tester subsystem. These signals include data on partial trips, partial trip enables, global trip, global bypass permissive, and automatic global bypass. The dynamic trip bus combines this data and determines the desired state of the reactor trip switchgear.

The dynamic trip bus interface panel incorporates controls for allowing each trip function to be placed in a manual partial trip, normal or manual bypass state. While the control is in the normal state, automatic operation of the partial trip function by the protection function is enabled. When the control is placed in either the trip or bypass state, the dynamic trip logic is forced to the desired partial trip or bypass condition regardless of the reactor trip subsystem output state.

7.1.2.2.4 Reactor Trip Switchgear Interface

The final stage of the dynamic trip bus provides the signal to energize the undervoltage trip attachment on each of the two division reactor trip switchgear breakers. Loss of the signal de-energizes the undervoltage trip attachments and results in the opening of the reactor trip breakers. An additional external relay is de-energized with the loss of the signal. The normally closed contacts of the relay energize the shunt trip attachments on each breaker at the same time that the undervoltage trip attachment is de-energized. This diverse trip

actuation is performed external to the protection and safety monitoring system cabinets. The reactor trip switchgear interface, including the trip attachments and the external relay, are within the scope of the protection and safety monitoring system. Separate outputs are provided for each breaker.

Testing of the interface allows trip actuation of the breakers by either the undervoltage trip attachment or the shunt trip attachment.

Figure 7.1-4 illustrates the reactor switchgear and manual trip interface.

7.1.2.2.5 Manual Reactor Trip

A manual reactor trip can be accomplished from either the main control room or the remote shutdown workstation by redundant momentary switches. The switches directly interrupt the power from the dynamic trip bus, actuating the undervoltage and shunt trip attachments. Figure 7.1-4 illustrates the implementation of the manual reactor trip function.

7.1.2.2.6 Engineered Safety Features Subsystems

The engineered safety features functions have also been divided into two microprocessor based subsystems for more reliable accident mitigation. Independence of the functionally diverse engineered safety features actuation functions is maintained from the integrated protection cabinet input circuitry, through the communications, to the engineered safety features actuation cabinets. This is accomplished by providing separate data links and transmitting and receiving hardware. The primary functions of the engineered safety features subsystems are to process inputs, calculate partial bistable actuations, combine the automatic actuation with the manual actuation and manual bypass data, and transmit the data to the engineered safety features actuation cabinets. To perform the protective function calculations, the subsystems require data from field sensors, and nuclear instrumentation sensors. The subsystems also use manual inputs from the main control room, the remote shutdown workstation, and locally mounted switches.

7.1.2.2.6.1 Manual Controls and Indications

To maintain independence between the engineered safety features subsystems, each subsystem uses a separate engineered safety features actuate/normal/bypass panel to implement the manual actuation and bypass of the engineered safety features functions. This panel provides the ability to place groups of sensor related engineered safety features functions in a forced actuate, normal (automatic), or bypass mode. Status indication is provided adjacent to the control. Each actuate/normal/bypass control allows an the engineered safety features function(s) to be manually actuated or bypassed by plant personnel. Should a failure be detected in the sensor or associated input circuitry, the individual function(s) can be actuated or bypassed rather than bypassing an entire division.

7.1.2.2.7 Communication Subsystem

The primary function of the communication subsystem is to provide information from the integrated protection cabinet to external systems. This includes outputs to the plant control system and the data display and processing system. Multiplexed information transfer is used to reduce the cabling between the systems. Fiber-optic data links are used to provide electrical isolation between the protection and safety monitoring system and the external systems. To obtain the information to be transmitted, the communication subsystem receives data from the other subsystems within the protection and safety monitoring system cabinets via internal electrical data links.

Analog inputs required for both control and protection functions are processed independently with separate input circuitry. The input signal is classified as safety-related and is, therefore, processed in the protection and safety monitoring system cabinet.

The integrated protection cabinets also provide data to the plant control system pertaining to signals calculated in the subsystems, and to the data display and processing system through an interface to the monitor bus.

7.1.2.2.7.1 Non-Process Inputs/Outputs

Four groups of non-process signals are provided to external systems via the optical data link originating in the communication subsystem. The subsystem informs the external systems of cabinet entry status, cabinet temperature, dc power supply voltages, and subsystem diagnostic status. This information is transmitted to the communication subsystem by the subsystems within the appropriate bay. Cabinet temperature sensing does not affect the safety-related function. The information is gathered for the sole purpose of analysis by external systems.

7.1.2.2.8 Automatic Tester Subsystem

The automatic tester subsystem provides a means of testing the operation of the integrated protection cabinet functions and verifying that the protection system setpoints and subsystem time response are within the system requirements. The automatic tester subsystem performs the test function while the division is bypassed. The verification level of the software executed by the subsystem is equivalent to the system being tested.

Prior to testing, the analog outputs of the automatic tester subsystem are calibrated. The test involves injection of simulated inputs and monitoring of the outputs to demonstrate that expected results are obtained. Testing is transparent to the other subsystems. Each subsystem executes only its normal functional software with input signals supplied by the automatic tester subsystem.

In addition to the testing function, the automatic tester subsystem monitors the failure and diagnostic information from the subsystems during normal operation, thus enhancing system maintenance of the integrated protection cabinets.

The design of the protection and safety monitoring system provides the ability to inject simulated input signals and to monitor data link outputs for the purpose of functional testing.

The automatic tester panel in each integrated protection cabinet provides operator interface capability for the automatic tester subsystem. In addition to switches, status lights and test jacks, the panel allows connection of a terminal and a printer to the system. These external devices provide enhanced status reporting and data logging. The automatic test panel provides a keyswitch that is used to manually enable automatic testing.

7.1.2.3 Engineered Safety Features Actuation Cabinets Subsystems

The engineered safety features actuation cabinet performs the following functions:

- Receive bistable data supplied by the four integrated protection cabinets and perform two-out-of-four voting on this data.
- Implement system-level logic using the input data from the protection and safety monitoring system cabinets and transmits the output to the protection logic cabinets via fiber-optic data links.
- Process manual system-level actuation commands received from the main control room.
- Provide redundant hardware capable of providing system-level commands to the division related portion of the protection logic cabinets.

The engineered safety features actuation cabinet provides redundant subsystems to perform the two-out-of-four voting of the bistable data acquired from an integrated protection cabinet. The results of this voting are provided to the protection logic cabinets for component actuation. The engineered safety features cabinet has the four following microprocessor based subsystems:

- Engineered safety features actuation subsystem 1
- Engineered safety features actuation subsystem 2
- Engineered safety features actuation cabinets automatic tester subsystem
- Engineered safety features actuation cabinets communication subsystem

Figure 7.1-5 illustrates the engineered safety features actuation cabinets.

7.1.2.3.1 Actuation Subsystems

The two engineered safety features actuation subsystems are redundant. The subsystems are functionally identical in both hardware and software. Each of the subsystems receives the engineered safety features bistable trip and bypass signals from each of the two engineered safety features microprocessor based subsystems which are located in the four integrated protection cabinets. They also receive the engineered safety features system-level engineered safety features manual actuation inputs from the main control room.

Appropriate voting logic is performed on the engineered safety features actuation and bypass signals received from the four integrated protection cabinets. The engineered safety features system-level manual actuation inputs are combined with the results of the voting logic. The resulting system-level commands are then transmitted to the protection logic cabinets via data highways.

Independent signal conditioning is performed on the data links received from the integrated protection cabinets on an engineered safety features subsystem basis. The functional diversity provided by the two engineered safety features subsystems located in the integrated protection cabinets is therefore maintained through to the actuation subsystems of the engineered safety features actuation cabinets.

7.1.2.3.2 Automatic Tester Subsystem

The engineered safety features actuation cabinets automatic tester subsystem performs the functional testing of the actuation subsystems. In addition, it monitors the subsystems of the engineered safety features actuation cabinets during normal operation similar to the automatic tester subsystem located in the integrated protection cabinets.

The engineered safety features actuation cabinets automatic tester subsystem performs a complete functional test of the engineered safety features actuation subsystems from the input circuitry, through to the data highway output, to the protection logic cabinets. The engineered safety features actuation cabinets automatic tester subsystem is capable of simulating the data link inputs and manual actuation inputs to the engineered safety features actuation cabinets by disconnecting the normal input signal and replacing it with a test signal. It monitors the data highway for correct system response to the input signals.

Each redundant engineered safety features actuation subsystem is tested individually.

The data link and contact input modules used by the subsystems include the capability of injecting simulated inputs for the purpose of testing. The data link output modules include the ability to monitor the transmitted signal.

Each engineered safety features actuation cabinet contains a test panel which provides man-machine interface capability to the engineered safety features actuation cabinets automatic tester subsystem. This panel contains switches and status lights for test initiation and monitoring. The panel also includes serial communication interfaces to the engineered safety features actuation cabinets automatic tester subsystem for connection to an external terminal and printer.

7.1.2.3.3 Communication Subsystem

The engineered safety features actuation cabinets communication subsystem serves as a central data collection point for the microprocessor based subsystems of an engineered safety features actuation cabinet. Information transfer is performed via data highways originating in the

actuation and tester subsystems. Once the data is organized, it is supplied to external systems via the monitor bus.

7.1.2.4 Protection Logic Overview

The protection logic illustrated in Figure 7.1-6 provides a distributed interface between the plant operator and the nonmodulating safety-related plant components. Nonmodulating control relates to the opening or closing of solenoid valves and solenoid pilot valves, and the opening or closing of motor-operated valves and dampers. The protection logic implements criteria established by the fluid systems designers for permissive and interlock logic applied to the component actuations. It also provides the plant operator with information on the equipment status, such as indication of component position (full closed, full open, valve moving), component control modes (manual, automatic, local, remote) or abnormal operating condition (power not available, failure detected).

The protection logic provides an interface between the engineered safety features component and system-level commands and nonmodulating engineered safety features actuating devices. The engineered safety features actuation cabinets in the protection and safety monitoring system perform the appropriate voting operation on the bistable signals and generate the system-level engineered safety features logic commands including the system-level manual commands. These system-level actuations are then sent to the protection logic cabinets over redundant data highways. The protection logic cabinets decode the system commands and actuate the final equipment through the interlocking logic specific to each component. Component-level actuation signals are sent from the main control room to the protection logic cabinets over redundant data highways. Component status is transmitted from the protection logic cabinets to the main control room over the same redundant data highways. Each protection logic cabinet is also capable of receiving and transmitting component status from and to other protection logic cabinets in the same division. Those components used for emergency shutdown can also be controlled from the remote shutdown workstation. The actuated safety-related components are grouped into four independent safety divisions. The architecture of one engineered safety features division within the protection logic is composed of the following equipment:

- One redundant logic bus
- One redundant main control room multiplexer
- One redundant remote shutdown workstation multiplexer
- Protection logic cabinets

The protection logic interfaces with the following external systems:

- The controls on the operator workstations in the main control room
- The controls on the remote shutdown workstation
- The output of the engineered safety features actuation cabinets (system-level engineered safety features signals, test signals, test feedback signals)

- The actuation devices (such as circuit breakers and solenoids) that control actuated equipment (such as valves)

- The position switches that indicate the operating state of the actuated equipment (such as valve open or closed limit switches)

- Other plant systems that control the actuated equipment or require status feedback from this equipment

7.1.2.4.1 Protection Logic Cabinets

The protection logic consists of four sets of protection logic cabinets, one set per engineered safety features division. The protection logic cabinets provide an interface between the engineered safety features actuation cabinets and the plant equipment that performs engineered safety feature functions. Each protection logic cabinet provides the following:

- Two functional logic subsystems
- Test/maintenance interface panel
- Three independent I/O busses
- I/O modules

Each protection logic cabinet has multiple microprocessor based subsystems as well as other standard cabinet equipment, such as power supplies, fans, and a blower. The rear of each protection logic cabinet contains I/O modules that provide the cabinet's external interfaces. These modules contain interfaces to data links, data highways, and plant components. The power interface cards perform two-out-of-three voting on the signals from the logic processors to determine the state of their outputs that control the plant components.

As illustrated in Figure 7.1-9, the protection logic cabinet has multiple processors connected to a single computer bus. This provides internal redundancy and additional fault tolerance within the protection logic cabinet as discussed in subsection 7.1.2.10. Each processor operates asynchronously. Bus contention is arbitrated by a combination of hardware and software. A failure of the hardware or software, which arbitrates bus contention, could result in a complete failure of one of the two processing functions performed within a single protection logic cabinet; however, this failure will have no effect since the other processing function will continue to operate. The I/O Bus Selector function provides the output cards with commands developed by the two functional processor cards which have not experienced the bus contention failure. If a protection logic cabinet fails, this failure affects only the equipment associated with a single mechanical train. Multiple mechanical trains of equipment are provided in AP600 so that the failure of equipment within a single equipment train is included in the design basis of the safety systems.

7.1.2.4.2 Logic Bus

In the protection logic equipment, the logic buses provide the communication interface between the engineered safety features actuation cabinets, the multiplexers, and the protection

logic cabinets. The protection logic contains two of these buses, one for each engineered safety features actuation subsystem. Each bus connects only the equipment (engineered safety features actuation cabinets, operator workstation multiplexer, and protection logic cabinets) in the same safety division. The logic bus in each division is composed of two data highways. The two highways are redundant in nature, and each uses fiber-optic cables as its transmission medium. One of the highways in a safety division connects together one of the redundant engineered safety features actuation subsystems in that division's engineered safety features actuation cabinet, one of the redundant halves of the multiplexers in that division, and the protection logic cabinets in that division. The other highway in the same division connects together the other engineered safety features actuation subsystem, the other half of the multiplexers, and the protection logic cabinets in that division.

7.1.2.5 Reactor Trip Switchgear

The reactor trip switchgear is used to initiate reactor shutdown. The reactor trip switchgear connects the electrical motive power, supplied from motor-generator sets, to the rod control system. The rod control system holds the control rods in position as long as electrical power is available. When the protection and safety monitoring system senses that established limits for safe operation of the plant have been, or are about to be, exceeded, a command is generated to de-energize the undervoltage trip device and energize the shunt trip device in the reactor trip switchgear breakers. This trips the breakers, disconnecting the power to the rod control system. When power is removed, the control rods drop by gravity into the reactor core, initiating the shutdown process.

The reactor trip switchgear is the final element in the protection and safety monitoring system which operates for reactor trip. There are four redundant safety divisions with each division containing two circuit breakers of the reactor trip switchgear (eight breakers total). As illustrated in Figure 7.1-7, the eight circuit breakers are arranged in a two-out-of-four logic configuration. The reactor trip switchgear includes associated or ancillary equipment and internal busbars. Breaker cells have steel barriers to completely encapsulate a breaker within its division and to provide physical separation between the breakers in different divisions.

7.1.2.6 Qualified Data Processing Cabinets

The qualified data processing cabinets, illustrated in Figure 7.1-8, are a redundant configuration consisting of sensors, qualified data processing cabinets, qualified displays, and qualified data processing I/O cabinets.

The qualified data processing cabinets perform the following functions:

- Provide safety-related data processing and display
- Provide the operator with sufficient operational data to safely shut the plant down in the event of a failure of the other display systems

- Provide qualified and nonqualified data to the monitor bus for use by other systems in the plant

- Process data for main control room and remote shutdown workstation display, and to meet Regulatory Guide 1.97 requirements

- Provide data to nonqualified emergency response facilities in conformance with NUREG-0696, the main control room, the plant computer, and other nonsafety-related devices

The I/O cabinets are microprocessor based, safety-related modular data gathering units. The I/O cabinet can receive inputs from process sensors and safety-related digital systems. The I/O cabinet consolidates the input data, performs conversions to process units, and formats the data for the data link transmission to the qualified data processing cabinets.

7.1.2.7 Main Control Room and Remote Shutdown Workstation Multiplexers

The protection and safety monitoring system contains eight multiplexers. One main control room multiplexer and one remote shutdown workstation multiplexer is associated with each of the four safety divisions. Each multiplexer consists of two redundant halves or subsystems. The multiplexers provide for transmission of component-level manual actuation signals from the main control room or remote shutdown workstation to the protection logic cabinets. The multiplexers also provide for transmission of component status information from the protection logic cabinet to the main control room and remote shutdown workstation.

The multiplexers communicate with soft control devices or operator interface modules in the main control room or the remote shutdown workstation over redundant fiber-optic data links. Subsection 7.1.3.4 provides additional discussion of the operation of the soft control devices. The transfer of control from the main control room to the remote shutdown workstation is accomplished using transfer switches as described in subsection 7.4.3.

Various "handshaking" signals are implemented for requests and responses between the soft controls and the multiplexers to verify the receipt and the validity of the messages.

7.1.2.8 Sensors

The protection and safety monitoring system monitors key variables related to equipment mechanical limitations, and variables directly affecting the heat transfer capability of the reactor. Some limits, such as the overtemperature ΔT setpoint, are calculated in the integrated protection cabinets from other parameters because direct measurement of the variable is not possible. This subsection provides a description of the sensors which monitor the variables for the protection and safety monitoring system. For convenience the discussions are grouped into the following three categories:

- Process sensors
- Nuclear instrumentation detectors

- Status inputs from field equipment

The inputs described are those required to generate the initiation signals for the protective functions. The use of each parameter is discussed in the sections that deal with each protective function. For example, reactor trip is discussed in Section 7.2 and engineered safety features actuation is described in Section 7.3.

7.1.2.8.1 Process Sensors

The process sensors are devices which measure temperature, pressure, fluid flow, and fluid level. Process instrumentation excludes nuclear and radiation measurements.

Additional information on these process variables is included as part of the description of each process system provided in other chapters. The process variables measured by the protection and safety monitoring system are listed in Sections 7.2, 7.3, and 7.5.

7.1.2.8.2 Nuclear Instrumentation Detectors

Three types of neutron detectors are used to monitor the leakage neutron flux from a completely shutdown condition to 120 percent of full power. The power range channels are capable of measuring overpower excursions up to 200 percent of full power.

The lowest range (source range) covers six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This generally is greater than two counts per second. The next range (intermediate range) covers eight decades. Detectors and instrumentation are chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) covers approximately two decades of the total instrumentation range. This is a linear range that overlaps the higher portion of the intermediate range. The neutron detectors are installed in tubes located around the reactor vessel in the primary shield. Detector types for these three ranges are:

- Source range - proportional counter
- Intermediate range - pulse fission chamber
- Power range - uncompensated ionization chamber

7.1.2.8.3 Equipment Status Inputs

Some inputs to the protection system are not measurements of process or nuclear variables, but are discrete indications of the status of certain equipment. Examples include manual switch positions, contact status inputs, and indications provided by valve limit switches.

7.1.2.9 Intercabinet Communications

Integrated Protection Cabinet to Integrated Protection Cabinet

Isolated fiber-optic data links are used for these communications links. The global trip subsystem in each integrated protection cabinet controls this communication link. These are standard one-way (simplex) communications used to transmit bistable trip status between integrated protection cabinets for use in two-out-of-four reactor trip logic.

Integrated Protection Cabinet to Engineered Safety Features Actuation Cabinet

Isolated fiber-optic data links in each integrated protection cabinet transmit bistable trip outputs to the engineered safety features actuation cabinet for use in engineered safety features actuation logic. These data links are one-way links that only transmit data to the engineered safety features actuation cabinets.

Engineered Safety Features Actuation Cabinet to Protection Logic Cabinets

Two redundant data highways are used for communications between the engineered safety features actuation cabinet and protection logic cabinets within each redundant safety division. Figure 7.1-6 shows this redundant data highway for a single safety division. This data highway provides for the transmission, by fiber-optics, of system-level actuation signals to the protection logic cabinets and for the transmission of component status information back to the engineered safety features actuation cabinet. The actuation signals to the protection logic cabinets are transmitted redundantly over the two data highways. The protection logic cabinets respond to an actuation signal from either data highway (one-out-of-two). Extensive testing and error checking on this data highway minimize erroneous actuation.

Protection Logic Cabinets to Multiplexers

Two redundant data highways are used for communication of component-level inputs from the main control room or remote shutdown workstation to the protection logic cabinets. Component status information is transmitted, by fiber-optics, from the protection logic cabinets to the main control room or remote shutdown workstation over the same redundant data highways. Figure 7.1-6 shows these data highways. Component status information on the data highways is also available to other protection logic cabinets within the same safety division for interlocking functions. The protection logic cabinets respond to a component-level actuation signal from either data highway. Extensive testing and error checking on this data highway minimize erroneous component-level actuations.

Integrated Protection Cabinet to Qualified Data Processing System

A data link is provided from each integrated protection cabinet to each qualified data processing cabinet. These data links are fiber-optic isolated, transmit only, from the integrated protection cabinets.

Integrated Protection Cabinet, Qualified Data Processing System, Engineered Safety Features Actuation Cabinet to Data Display and Processing System

A data link is provided from each integrated protection cabinet, qualified data processing cabinet, and engineered safety features actuation cabinet to the monitor bus of the data display and processing system. These data links are fiber-optic isolated, transmit only, to the monitor bus.

7.1.2.10 Fault Tolerance, Maintenance, Test, and Bypass

The protection and safety monitoring system provides a high degree of reliability and fault tolerance. This capability is demonstrated by the following design features:

- Two-out-of-four coincidence logic on reactor trip and most engineered safety features actuations provides that any failure in a single protection channel or safety division cannot cause a spurious reactor trip or spurious system-level engineered safety features actuation. This same two-out-of-four logic also provides that any failure in a single protection channel or safety division cannot prevent a required reactor trip or system level engineered safety features actuation from occurring. This provides tolerance against failures ranging from the failure of a single instrument or component, to the complete failure of an entire integrated protection or engineered safety features actuation cabinet.

- Reactor trip and engineered safety features actuation logic reverts to two-out-of-three coincidence logic if one channel is bypassed or in test. Therefore a single failure while in test cannot cause a spurious reactor trip or spurious system-level engineered safety features actuation. This same two-out-of-three logic also provides that any failure in a single protection channel or safety division cannot prevent a required reactor trip or system-level engineered safety features actuation from occurring. The logic permitting placing of channels in a bypass condition is denoted by "2/4-BYP" on the functional diagrams. The following table summarizes the automatic voting logic associated with the number of inputs bypassed.

Number of Inputs Bypassed	Number of Remaining Inputs to Result in a Reactor Trip or Safety Features Actuation
0	two-out-of-four (2/4)
1	two-out-of-three (2/3) (alarmed)
2	one-out-of-two (1/2) (alarmed)
3	automatic trip or actuation
4	automatic trip or actuation

The bypass logic allows the system to meet the single failure criterion with one or two channels bypassed for testing or maintenance.

- The reactor trip logic provided in the integrated protection cabinets also processes the manual system-level inputs involved in the reactor trip function. Section 7.2 provides further detail of the manual trip function.

  The voting logic for reactor trip functions is contained within each integrated protection cabinet. The reactor trip breakers operate on a de-energize-to-trip principle.

- Engineered safety features actuation logic is performed redundantly in each engineered safety features actuation cabinet, as shown in Figure 7.1-5. Redundant microprocessor based subsystems perform this logic so that a component failure related to one subsystem cannot affect the other redundant subsystem. The system-level actuation outputs are transmitted to the protection logic cabinets over two redundant data highways. A single data highway failure cannot prevent engineered safety features actuation. Extensive error checking is performed on these data highways to minimize failures from causing spurious actuation.

- Component-level logic, performed within the protection logic cabinets, is triple redundant, as illustrated in Figure 7.1-9. Four redundant logic processor boards are provided along with two data highway controller boards. Two logic processor boards are associated with each data highway controller board. The logic processors are programmed to respond to actuation signals received from the data highways. Failure of one data highway or one data highway controller board does not prevent component-level actuations. Extensive error checking on the data highways is provided to minimize data highway failures from generating spurious engineered safety features component-level actuations. The component actuation outputs from the logic processors are combined with the power interface cards in a two-out-of-three voting logic. This prevents the failure of a single logic processor from causing spurious actuation or preventing a required actuation.

During maintenance, these same features that provide for fault tolerance allow the system to continue to operate with one channel or certain boards out of service. Any single integrated protection cabinet, engineered safety features actuation cabinet, or transmitter associated with one trip or actuation channel may be taken out of service for maintenance without plant shutdown. The data highways connecting the engineered safety features actuation cabinets, protection logic cabinets, and multiplexers are redundant. One of the redundant highways may be out of service, for maintenance, without directly causing plant shutdown. Since the logic processors and data highway controllers in the protection logic cabinets are redundant, one logic processor or data highway controller can be out of service, for maintenance, while the overall system remains operational.

Functionally diverse protective functions in an integrated protection cabinet are implemented in separate microprocessor based subsystems. When the same process input is required by

more than one subsystem, the analog signal is run separately to analog/digital input converters in each subsystem.

7.1.2.11 Isolation Devices

Isolation devices are used to maintain the electrical independence of divisions, and to see that no interaction occurs between nonsafety-related systems and the safety-related system.

Isolation devices are incorporated into selected data links to maintain division independence. Isolation devices serve to prevent credible faults (such as open circuits, short circuits, or applied credible voltages) in one circuit from propagating to another circuit.

Optical coupling offers improved physical and electrical isolation and separation since it eliminates electrically conductive paths between the receiving and transmitting terminal.

7.1.2.12 Built-in Test Capabilities

The safety-related instrumentation facilitates periodic testing from the sensor inputs of the protection and safety monitoring system through to the actuated equipment. Testing is accomplished through a series of overlapping sequential tests with the majority of the tests capable of being performed with the plant at full power. Where testing final equipment at power would upset plant operation or destroy equipment, provisions are made to test the equipment at reduced power or when the reactor is shut down.

With the exception of operating the final actuators, the test philosophy is to manually initiate the automatic test sequence, with the test itself proceeding with no operator intervention. Each integrated protection and engineered safety features actuation cabinet is furnished with an automatic tester. The automatic tester provides for injection of reference analog signals into cabinet circuitry, verification of the accuracy of setpoints and other constants, and verification that proper signals appear at other locations in the system.

The test begins by checking the analog-to-digital converters over their range of operation, using injected reference signals. Verification of the signal processing algorithms is made by exercising the test signal sources and observing the results up to, and including, the attainment of a channel partial trip or actuation signal at the power interface. The tester automatically places the voting logic associated with the channel function under test in bypass.

The overlapping test sequence continues by inputting digital test signals at the output side of the threshold functions, in combinations necessary to verify the voting logic. Some of the input combinations to the coincidence logic cause outputs such as reactor trips and engineered safety features initiation. The reactor trip circuit breakers are arranged in a two-out-of-four logic configuration, such that the tripping of the two circuit breakers associated with one division does not cause a reactor trip. This circuit breaker arrangement is illustrated in Figure 7.1-7. To reduce wear on the breakers through excessive tripping, and to avoid a potential plant trip resulting from a single failure while testing is in progress, the reactor trip channel

under test is bypassed. This bypass causes the trip logic to revert to two-out-of-three in the remaining reactor trip divisions. Testing of the circuit breakers is performed separately.

The automatic tester does not test the engineered safety features actuators. This portion of the test may be accomplished by using component-level actuation signals. These signals enter the protection logic cabinet through the data highways. For those final devices that can be operated at power, without upsetting the plant or damaging equipment, the test is performed by actuating the manual actuation control which causes the device to operate. Position switches on the device itself send a signal back to the protection logic cabinet, where it is transmitted to the main control room for display purposes. The display verifies that the manual command is successfully completed, thus verifying operability of the final device. For those devices which cannot be tested at power without damage or upsetting the plant, the manual test is conducted from test switches at the engineered safety features actuation cabinet. These switches block device actuation. Continuity of the wiring up to the actuation device is verified. Operability of the final equipment is demonstrated at reduced power or at shutdown, depending on the equipment.

Operation procedures prohibit testing two divisions at the same time. There are no built-in interlocks to prevent simultaneous testing of two integrated protection cabinets. However, the use of bypasses by the tester provides that the protection and safety monitoring system cannot be placed in an unsafe condition if the procedure prohibiting simultaneous testing is violated. For example, testing two divisions results in two bypasses, which causes the voting logic to revert to a one-out-of-two coincidence for the remaining two unbypassed divisions. Attempting to test three or four divisions at the same time causes a plant trip. The operational procedure restricting simultaneous testing of two or more divisions is for operability reasons to avoid unnecessary trips.

In addition to periodic tests, the system performs error detection and data link testing as part of its normal operation. Where practical, the on-line error detecting features are designed to automatically place the channel in which the error was detected into a trip or bypass state (either by direct bypass or reconfiguration). When a channel is automatically placed into a trip state, the operator has the option to subsequently place that channel in a bypass state. If the automatic configuration of the channel is not practical, the on-line error detecting feature causes alarm annunciation to the operator.

7.1.2.13 Safety-Related Display Instrumentation

Safety-related display instrumentation provides the operator with information to determine the effect of automatic and manual actions taken following reactor trip due to a Condition II, III, or IV event as defined in Chapter 15. This instrumentation also provides for operator display of the information necessary to meet Regulatory Guide 1.97. A description of the equipment used to provide this function is provided in subsection 7.1.2.6. A description of the data provided to the operator by this instrumentation is provided in Section 7.5.

7.1.2.14 Auxiliary Supporting Systems

The safety-related system equipment is supported by the supply of uninterruptable electrical energy. This electrical power is supplied by the Class 1E dc and UPS system discussed in Chapter 8.

7.1.2.15 Verification and Validation

[*Adequacy of the hardware and software is demonstrated for the protection and safety monitoring system through a verification and validation (V&V) program. Details on the verification and validation program are provided in WCAP-13383 (Reference 4).*]* The software development process which is documented in this document is consistent with the following standards:

- ANSI/IEEE ANS-7-4.3.2 (1993); "Application Criteria for Programmable Digital Computer Systems in Safety Systems for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations"
- IEC 880-1986; "Software for Computers in the Safety Systems for Nuclear Power Generating Stations"
- IEEE 828-1983; "IEEE Standard for Software Configuration Management Plans"
- IEEE 829-1983; "IEEE Standard for Software Test Documentation"
- IEEE 830-1984; "IEEE Standard for Software Requirements Specifications"
- IEEE 1012-1986; "IEEE Standard for Software Verification and Validation Plans"
- IEEE 1042-1987; "IEEE Guide to Software Configuration Management (ANSI)"

[*WCAP-13383 provides a planned design process for hardware and software development during the following life cycle stages:*

- *Design requirements phase*
- *System definition phase*
- *Hardware and software development phase*
- *System test phase*
- *Installation phase*

WCAP-13383 also provides for the use of commercial off-the-shelf hardware and software through a commercial dedication process.]* Control of the hardware and software during the operational and maintenance phase is the responsibility of the Combined License applicant as described in subsection 13.5.1.

*NRC Staff approval is required prior to implementing a change in this material; see DCD Introduction Section 3.5.

7.1.3 Plant Control System

The plant control system is a nonsafety-related system that provides control and coordination of the plant during startup, ascent to power, power operation, and shutdown conditions. The plant control system integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for required normal and off-normal conditions. The plant control system also provides control of the nonsafety-related decay heat removal systems during shutdown. The plant control system accomplishes these functions through use of the following:

- Rod control
- Pressurizer pressure and level control
- Steam generator water level control
- Steam dump (turbine bypass) control
- Rapid power reduction

The plant control system provides automatic regulation of reactor and other key system parameters in response to changes in operating limits (load changes). The plant control system acts to maximize margins to plant safety limits and maximize the plant transient performance. The plant control system also provides the capability for manual control of plant systems and equipment. Redundant control logic is used in some applications to increase single-failure tolerance.

The plant control system includes the equipment from the process sensor input circuitry through to the modulating and nonmodulating control outputs as well as the digital signals to other plant systems. Modulating control devices include valve positioners, pump speed controllers, and the control rod equipment. Nonmodulating devices include motor starters for motor-operated valves and pumps, breakers for heaters, and solenoids for actuation of air-operated valves. The control cabinets contain the process sensor inputs and the modulating and nonmodulating outputs. The plant control system also includes equipment to monitor and control the control rods.

The functions of the plant control system are performed by system assemblies including:

- Distributed controllers
- Signal selectors
- Process bus multiplexers
- Operator controls and indication
- Process bus
- Rod control system
- Rod position indication
- Rod drive motor-generator sets
- Pressurizer heater control interface

Figure 7.1-10 provides an illustration of the plant control system.

7.1.3.1 Distributed Controllers

Each distributed controller processes inputs, performs system-level and component-level control calculations, provides an operator interface to the controlled components, transmits control signals to discrete, modulating, and networked interfaced control components, and provides plant status and plant parameter information to the process bus.

The distributed controllers receive process inputs and implement the system-level logic and control algorithms appropriate for the plant operating mode. The distributed controllers receive process inputs from, and transmit process control outputs to, the actuated components. The distributed controller also transmits and receives process signals via the process bus. The process bus facilitates the receipt of process signals from the protection and safety monitoring system via the signal selector, facilitates the transmission of process signals to the monitor bus via the gateway shown on Figure 7.1-1, and provides for two-way communication between the individual distributed controllers via the process bus. The process bus also provides for two-way communication between the distributed controllers and the main control room and remote shutdown workstation via the multiplexers.

Control functions are distributed across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functions performed by other controllers. The major control functions which are implemented in different distributed controllers include reactor power control, feedwater control, pressurizer control, and turbine control.

7.1.3.2 Signal Selectors

Redundant signal selectors provide the plant control system with the ability to obtain inputs from the integrated protection cabinets in the protection and safety monitoring system. The signal selector function maintains the independence of the plant control system and the protection and safety monitoring system. The signal selectors select those protection system signals that represent the actual status of the plant and reject erroneous signals. Therefore, the control system does not cause an unsafe control action to occur even if two of four redundant protection channels are degraded by random failure or by being bypassed for test or maintenance.

Each signal selector receives data from each of the redundant divisions of the integrated protection cabinets. The data is received from each integrated protection cabinet on a serial data link via fiber-optic cable.

The signal selectors provide validated process values to the plant control system via the process bus. They also provide the validation status, the average of the valid process values, the number of valid process values, an alarm (if one process value has been rejected), and another alarm (if two process values have been rejected).

For the logic values received from the protection and safety monitoring system, such as permissives, the signal selectors perform voting on the logic values to provide a valid logic

value to the plant control system via the process bus. They also provide the validation status, the number of valid logic values, an alarm if one logic value differs from the voted value, and another alarm if two logic values differ from the voted value. Each signal selector provides information to the process bus.

The redundant signal selectors receive identical data from the integrated protection cabinets and perform identical selection algorithms. Each selector provides validated data to one of the redundant highways of the process bus. When there is no failure of either signal selector or either highway, the distributed controllers are free to use data from either of the signal selectors via the appropriate highway. The signal selector subsystem redundancy serves two purposes; it protects against a failure disrupting the control system, and it provides the capability to remove one of the selectors from service for testing while maintaining normal control using data from the other selector.

7.1.3.3 Process Bus Multiplexers

The process bus multiplexers provide for manual system-level and component-level control capability from the main control room and the remote shutdown workstation. The process bus multiplexers receive manual control commands from the soft and dedicated control devices and transmits these commands onto the process bus. These control commands may then be used by the distributed controllers as manual control inputs. Signals used for indication to the operator are also returned to the main control room and remote shutdown workstation. The appropriate indication signals are transmitted onto the process bus by the distributed controllers. The process bus multiplexers receive these indication signals from the process bus and transmits these indication signals to the indicating devices for use by the plant operators. Redundant process bus multiplexers are provided so that a single multiplexer can be out of service without disrupting operation.

7.1.3.4 Operator Controls and Indication

The plant control operator interface is a set of soft control devices that replace conventional switch/light or potentiometer/meter assemblies used for operator interface with control systems. These soft control devices provide consistent operator interfaces for the plant control system. The soft controls are located on each operator workstation and the remote shutdown workstation. These soft controls are linked to the process bus multiplexers by individual data links. The data links use fiber optic cable and are provided with error detection capability. Incoming data consists of messages received from operator display and field devices. Outgoing messages consists of messages which are sent to the appropriate control device to await operator confirmation. The operator confirmation function is provided by a device which is electrically separate from the soft control device. Each soft control device can control safety-related and nonsafety-related equipment; however, it is designed such that it can only communicate with a single division at any one time.

The implementation of the soft controls is consistent with the following functional requirements:

- The soft control function does not affect the electrical or functional isolation of the safety-related and nonsafety-related equipment. This isolation is maintained upon a single failure of any equipment performing or supporting the soft control function.

- Failure of the operator displays does not prevent an operator from being able to safely shutdown the plant.

When the operator desires to operate a component, the graphical operator display which is indicating the component status is presented on the operator control console. This results in a message being sent to the soft control device. The soft control device then displays the appropriate control template. The operator then selects the desired control action on the template. After the operator verifies that the desired control action is properly selected, the operator actuates the confirmation device, causing the selected control action to be transmitted to the control device.

7.1.3.5 Process Bus

The process bus is a collection of redundant data highways that support both periodic and aperiodic data transfers of nonsafety-related signals and data. Periodic transfers consist of process data that is broadcast over the process bus at fixed intervals and is available to all destinations. Aperiodic data transfer is generally used for messages or file transfers. The process bus is a fiber distributed data interface network. This token-passing network operates at 100 Mb/s using fiber optic cables.

The process bus provides communications among the distributed controllers, the signal selectors, the process bus multiplexers, and the rod control system cabinets. A process bus gateway, shown on Figure 7.1-1, provides for the transmission of selected process bus data to the monitor bus.

7.1.3.6 Rod Control System

The primary means of regulating the reactor power and power distribution is to position clusters of control rods in the reactor core using the rod control system.

The control rods are moved into and out of the reactor core by means of electromagnetic jacking mechanisms, called control rod drive mechanisms, located on the reactor vessel head. Each control rod drive mechanism consists of two gripper mechanisms, one stationary and one movable, that hold a notched driveline attached to the upper end of the control rod. The movable gripper is housed in an armature that allows vertical travel over 5/8 inch. The grippers and the lift armature are controlled by coils mounted external to the mechanism, concentric with the rod driveline. By controlling the sequence of energizing these coils, the mechanism can be made to step into, or out of, the reactor in increments of 5/8 inch. The rod control equipment provides this sequence control.

The control rods are arranged into symmetrical groups. The groups of control rods are divided into two categories: shutdown rods that are normally held fully withdrawn from the reactor, and control rods that are positioned to some intermediate insertion. In addition, there is a subcategory of control rods (low worth gray rods). If a rapid shutdown is necessary, the control, shutdown, and gray rods are dropped into the reactor by de-energizing their drive mechanisms.

Interlocks are provided to prevent the motion of the control rods outside of planned sequences.

7.1.3.6.1 The Rod Control Cabinet Architecture

The rod control cabinets consist of a logic cabinet and sufficient power cabinets for the control rods. The power cabinets are of two types: the moving cabinet and the selecting cabinets.

The logic cabinet provides the main intelligence of the system. Group selection and interlocking functions are performed by the microcomputer subsystems within this cabinet. The power cabinets are divided into sets. Within each set of power cabinets there is a moving cabinet, which contains the current regulating equipment for the lift coils. Each set of power cabinets also contains several selecting cabinets, containing the gripper coil current regulators and the control rod drive mechanism select multiplex switches. The moving cabinets provide dc current pulses for the lift coils in the moving group of rods. The selecting cabinets provide the dc current for the gripper coils, and also switch the lift and gripper coil currents to their associated control rods. Each selecting cabinet contains the circuits for two groups of rods. Only one group within a power cabinet set is permitted to move at a given time except during bank overlap.

A feature that is specific to the selecting cabinets is the insurance bus. This bus provides an alternative means to energize the holding capability of the control rod drive mechanism. Stationary coils can extract energy from the insurance bus.

The rod drive motor-generator sets provide the power to the control rod drive mechanisms through the reactor trip switchgear. The rod drive motor-generator sets are included in the plant control system. The safety-related reactor trip switchgear is included in the plant protection and safety monitoring system.

7.1.3.7 Rod Position Indication

The position of each control rod is continuously monitored by the rod position indication system. This information is detected by the rod position detector assemblies. The signals from the detectors are processed by the data cabinets and transmitted to the distributed controllers over the process bus. The distributed controllers further processes the rod position information and transmits this information to the monitor bus via the process bus gateway.

7.1.3.8 Rod Drive Motor-Generator Sets

The rod drive motor-generator sets supply power to the rod control equipment. This subsystem includes two motor-generator sets with flywheels and one control cabinet. Each motor-generator is a three-phase induction motor, direct-coupled to a flywheel, and a synchronous alternator.

During normal operating conditions, both motor generator sets are operating in parallel and equally sharing the total load demand. Each motor-generator set is capable of supplying the entire load requirements when the other set is out of service.

7.1.3.9 Pressurizer Heater Control Interface

The pressurizer heater control interface controls the power input to the resistance heaters located in the pressurizer. Most of the pressurizer heater banks are controlled in a discrete manner. The bank is either turned completely on or turned completely off. In these cases, the heater bank control interface consists of circuit breakers.

One of the pressurizer heater banks is controlled by a modulating controller. This controller is a thyristor power controller that provides time proportioning control of the ac power input to the pressurizer heaters. In time proportioning control, the thyristors are on for a controlled number of half cycles, each being fired at the instant of zero line voltage. The on and off times are varied to provide a variable duty cycle.

7.1.4 Identification of Safety Criteria

7.1.4.1 Design Basis for Safety Systems

The design bases presented in the following subsections apply to the safety-related system instrumentation described in subsection 7.1.1. Specific design bases information for protective functions are given in Section 7.2 for reactor trip and Section 7.3 for engineered safety features. The design bases presented include those addressed by Section 3 of IEEE 279 (Reference 5).

7.1.4.1.1 Design Basis: Generating Station Conditions Requiring Protective Actions (Paragraph 1 of Section 3 of IEEE 279-1971)

The safety-related system described in subsection 7.1.1 is designed to protect the health and safety of the public by limiting the release of radioactive material during Conditions II, III, and IV events to acceptable limits, as defined in Chapter 15.

To facilitate the design of the protection system, a number of specific limits on certain process and design variables have been chosen which, if met, imply that the radioactive material release limits can be met with a high degree of confidence. These specific limits are defined on an accident by accident basis in Chapter 15.

7.1.4.1.2 Design Basis: Variables Required to be Monitored for Protective Action and Their Minimum Performance Requirements (Paragraphs 2 and 9 of Section 3 of IEEE 279-1971)

The variables required to be monitored for reactor trip and their ranges, accuracies, and response times are discussed in subsection 7.2.1.2.2. The applicability of these trips to design basis transients and accidents is also presented in that subsection.

The variables required to be monitored for engineered safety features actuation and their ranges, accuracies, and response times are discussed in subsection 7.3.1.5.2.

The variables required to be monitored for post-accident monitoring are discussed in Section 7.5.

The design conforms to Paragraph 4.8 of IEEE 279-1971.

7.1.4.1.3 Design Basis: Spatially Dependent Variables (Paragraph 3 of Section 3 of IEEE 279-1971)

The spatially dependent variables required to be monitored for the safety-related system are discussed in subsection 7.2.1.2.3.

7.1.4.1.4 Design Basis: Protection During Various Reactor Operating Modes (Paragraph 4 of Section 3 of IEEE 279-1971)

The safety-related system is designed so that protective functions are initiated and accomplished during various reactor operating modes. The following specific design bases apply.

Protection System Channel Bypass During Test or Maintenance

The safety-related system is designed to permit the bypass for maintenance, test, or repair of any one protection channel in the group of channels monitoring a selected variable. This bypass is accomplished during power operation without causing initiation of a protective function. The system also meets the single failure criterion while permitting power operation for an indefinite period of time with one channel of the selected variable bypassed.

With one channel bypassed, the system permits the bypass of a second channel in the group monitoring the same variable. In this mode, the failure of a third channel in the group may result in a protective function initiation. The system meets the single failure criterion with two channels of the selected variable bypassed by reverting to a one-out-of-two logic. Operation with two channels of one variable bypassed is alarmed.

The attempt to bypass three or more channels monitoring the same variable results in initiation of the protective functions associated with that variable.

The capability for channel bypass or removal from operation conforms to Paragraphs 4.11 through 4.14 of IEEE 279-1971. Conformance is discussed in subsections 7.1.4.2.11 through 7.1.4.2.14.

Protection System Blocks, Interlocks, and Permissives for Defined Reactor Operating Modes

Where operating requirements necessitate automatic or manual block of a protective function, the block is automatically removed whenever the appropriate permissive conditions are not met. Devices used to achieve automatic removal of the block of a protective function are considered part of the safety-related system and, as such, are designed in accordance with the criteria in this section.

Interlocks are discussed in Sections 7.2, 7.3, and 7.6. The safety analyses demonstrate that even under conservative critical conditions for design basis accidents, the protective system provides confidence that the plant is put into and maintained in a safe state following a Condition II, III or IV accident. Therefore, the protective systems meet IEEE 279-1971 and are entirely redundant and separate, including permissives and blocks. Blocks of a protective function are automatically cleared when the protective function is required to function according to Paragraphs 4.11, 4.12 and 4.13 of IEEE 279-1971. Subsections 7.1.4.2.11 through 7.1.4.2.13 provide further detail on this conformance.

Multiple Setpoints Used During Defined Reactor Operating Modes

Setpoints in the integrated protection cabinet are not more restrictive as a function of operational mode.

Access to Protection System Bypasses, Blocks, and Setpoints

The system provides for administrative control over access to the means for manually bypassing protection channels and for manually blocking protective functions. Administrative control of access is provided to setpoint adjustments, channel calibration adjustments, and test points.

The system meets Paragraphs 4.14 and 4.18 of IEEE 279-1971. Conformance is discussed in subsections 7.1.4.2.14 and 7.1.4.2.18.

7.1.4.1.5 Design Basis; Determination of Protective Action Setpoints (Paragraphs 5 and 6 of Section 3 of IEEE 279-1971)

The safety-related system automatically initiates appropriate protective action when a condition monitored by the system reaches a preset level.

The design conforms to Paragraph 4.1 of IEEE 279-1971. Conformance is discussed in subsection 7.1.4.2.1.

7.1.4.1.6 Design Basis: Protection Against Natural Phenomena and Unusual Events (Paragraphs 7 and 8 of Section 3 of IEEE 279-1971)

The ability to initiate and accomplish protective functions is maintained during and following natural phenomena described in Chapter 2 as credible to the plant, such as earthquakes, tornados, hurricanes, floods, and winds. Plant safety is provided despite degraded conditions caused by internal events such as fire, flooding, explosions, missiles, electrical faults, and pipe whip as discussed in Chapter 3.

Equipment is environmentally qualified to meet the accident conditions through which it operates to mitigate the consequences of the accident. Equipment is seismically qualified to meet design basis earthquake levels.

The digital equipment design has additional design margin to accommodate a loss of the normal HVAC. Safety-related digital equipment is protected by the passive HVAC upon any failure or degradation of the active HVAC. The passive HVAC limits the rate of temperature rise in the rooms containing the digital equipment. The cabinets containing the digital equipment are provided with temperature sensors which provide an alarm if internal cabinet temperatures reach an excessive value. In addition, the equipment is qualified at a temperature which envelope the worse case temperature for which the equipment must continue to function. Details of the equipment design are provided in WCAP-13382 (Reference 3).

Electromagnetic design, testing, and qualification of the digital equipment is performed in accordance with guidance provided in the following standards:

- Electrostatic discharge (ESD) immunity in accordance with IEC 1000-4-2
- Radio frequency interference (RFI) immunity in accordance with IEC 1000-4-3 and MIL-STD-461C and MIL-STD-462
- Electrical fast transient (EFT) immunity in accordance with IEC 1000-4-4
- Surge immunity in accordance with IEC 1000-4-5, IEEE C62.45-1992, and ANSI/IEEE C37.90.1-1989
- RFI emission in accordance with MIL-STD-461C and MIL-STD-462
- Conducted RFI immunity in accordance with MIL-STD-461C and MIL-STD-462
- Grounding and shielding in accordance with IEEE 1050-1989

An example of the manner in which these standards are used in the testing of the digital equipment is provided in WCAP-11340 (Reference 11).

The design conforms to Paragraphs 4.3, 4.4, and 4.5 of IEEE 279-1971. Conformance is discussed in subsections 7.1.4.2.3 through 7.1.4.2.5.

7.1.4.1.7 Design Basis: Protection Against Equipment Malfunctions

The ability of the safety-related system to initiate and accomplish protective functions is maintained despite credible equipment malfunctions within the safety-related system. The safety system meets the single failure criterion. The following specific design bases apply:

- A single credible failure within the safety-related system does not prevent initiation or execution of a protective function, even when channels are intentionally bypassed for test or maintenance.

- Where signals are derived from protection channels for control, no credible single failure in the protection channel causes a control system action requiring protective action by the redundant channels monitoring the same variable.

- Where signals are derived from protection channels for nonsafety systems, no credible failure in the nonsafety-related system prevents the protection system from meeting its performance requirements.

- No single failure within the protection system causes a Condition II event to progress to a Condition III event, or a Condition III event to progress to a Condition IV event.

The system meets the single failure criterion, as established by Paragraph 4.2 of IEEE 279-1971. Conformance to this paragraph is discussed in subsection 7.1.4.2.2. Prevention of control system interaction with the protection system is designed according to Paragraph 4.7 of IEEE 279-1971. Conformance to this requirement is discussed in subsection 7.1.4.2.7.

7.1.4.1.8 Miscellaneous Design Bases

Manual Actuation of Protective Functions

Means are provided in the main control room for manual initiation of protective functions at the system-level. Manual actuation relies on minimum equipment and, once initiated, proceeds to completion unless deliberate operator intervention is taken. Failure in the automatic initiation portion of a system-level function does not prevent the manual initiation of that function.

The system conforms with Paragraphs 4.16 and 4.17 of IEEE 279-1971. Conformance is discussed in subsections 7.1.4.2.16 and 7.1.4.2.17.

Physical Identification of Protection System Equipment

To verify that the design bases given in this section can be applied in the design, construction, maintenance, and operation of the plant, safety-related systems equipment is identified distinctly as being in the protection system. Markings are different for each redundant division of the safety-related system.

The design conforms to Paragraphs 4.22 of IEEE 279-1971. Conformance is discussed in subsection 7.1.4.2.22.

Capability for Checks, Test, Calibration, and System Repair

The system permits checking the operational availability of each input sensor to the protection system during reactor operation.

Capability is provided for testing and calibrating the channels of the protection system.

The system facilitates the diagnosis, location, and repair or adjustment of malfunctioning components.

The system conforms to Paragraphs 4.9, 4.10, and 4.21 of IEEE 279-1971. Conformance is discussed in subsections 7.1.4.2.9, 7.1.4.2.10, and 7.1.4.2.21.

Information Read-Out

The system permits identification of protective actions down to the channel level. The system is designed to provide the operator with information on the status of safety-related system equipment.

The design conforms to Paragraphs 4.19 and 4.20 of IEEE 279-1971. Conformance is discussed in subsections 7.1.4.2.19 and 20.

Conformance With Industry Standards

[*The instrumentation and control systems are designed in accordance with guidance provided in applicable portions of the following standards. The portions of the standards which are considered to be applicable are the portions of the standards which apply to instrumentation and control systems performing protection and control functions in an industrial environment:*

- *IEC 68-2-1, 1974; "Basic Environmental Testing Procedures"*
- *IEC 68-2-6, 1982; "Basic Environmental Testing Procedures, Part 2.1 Tests - Tests Fc: Vibration (Sinusoidal)"*
- *IEC 1000-4 Series; "EMC Part 4: Testing and Measurement Techniques"*
- *IEC 1000-4-2, 06/94; "Section 2: Electrostatic Discharge Immunity Test"*
- *IEC 1000-4-3, 08/94; "Section 3: Radiated, Radio-frequency, Electromagnetic Field Immunity Test"*
- *IEC 1000-4-4, 07/94; "Section 4: Electrical Fast Transient/Burst Immunity Test"*

- *IEC 1000-4-5, 09/94; "Section 5: Surge Immunity Test"*
- *IEC 1000-4-6, 05/94; "Section 6: Immunity to Conducted Disturbances, Induced by Radio-Frequency Fields"*
- *IEEE C62.45-1992; "IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits"*
- *IEEE C37.90.1-1989; "IEEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems"*
- *IEEE 1050-1989; "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations"*
- *MIL-STD-461C; "Electromagnetic Emission and Susceptibility Requirements for Control of Electromagnetic Interference"*
- *MIL-STD-462; "Measurement of Electromagnetic Interference Characteristics"]**

7.1.4.2 Conformance of the Safety System Instrumentation to Applicable Criteria

The safety-related system instrumentation described in subsection 7.1.1 is designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power. Applicable General Design Criteria are listed in Section 3.1, NRC Regulatory Guides in subsection 1.9.1, and Branch Technical Positions in subsection 1.9.2. Industry Standards are cited as references.

The instrumentation and control portion of the safety-related system is discussed in subsections 7.1.4.2.1 through 7.1.4.2.22. The topics are listed in the same order as they appear in Section 4 of IEEE 279-1971. That standard provides the design bases of the instrumentation and control portion of the safety system. Other criteria related to the IEEE 279-1971 requirements are also identified.

7.1.4.2.1 Conformance to General Functional Requirements (Paragraph 4.1 of IEEE 279-1971, GDC-13, GDC-15, Regulatory Guide 1.105)

The safety-related system automatically initiates appropriate protective action whenever a condition monitored by the system reaches a preset value. Reactor trip functions are discussed in Section 7.2. Engineered safety features are discussed in Section 7.3. Also provided in those sections are the ranges, and typical accuracies and response times for each variable used in generating a protective action.

The preset values are verified by calculating total instrument channel errors and determining that the difference between the preset value and the safety analysis limit for that function equals or exceeds the calculated value.

*NRC Staff approval is required prior to implementing a change in this material; see DCD Introduction Section 3.5.

Range selection for the instrumentation covers the expected range of the process variable monitored. The protection system is designed so that trip setpoints do not require process transmitters to operate within five percent of the high and low end of their calibrated span or range. Functional requirements established for every channel in the protection system stipulate the maximum allowable accuracy. The protection channels have the capability to provide, and are tested to verify, that the characteristics throughout the entire span are acceptable and meet functional requirements.

7.1.4.2.2 Conformance to the Single Failure Criterion (Paragraph 4.2 of IEEE 279-1971, IEEE 379-1988, Regulatory Guide 1.53)

A credible single failure within the protection system does not prevent the initiation or accomplishment of a protective function at the system level.

Redundancy is designed into the safety system to provide that system performance requirements are met even if the safety-related system is degraded by a single failure. Redundancy begins with the sensors monitoring the variables and is carried through the signal processing and actuation electronics. Redundant actuations are also provided. Subsections 7.1.1 and 7.1.2 describe the redundant nature of the safety system architecture. Two or more diverse functions initiate most protective actions. Diversity of protective functions is discussed in Section 7.2 for reactor trip, and in Section 7.3 for engineered safety features actuation.

Isolation devices are incorporated into data links that connect redundant divisions or carry signals to nonsafety systems. The isolation devices are tested to verify that credible faults, such as physical damage, short circuits, open circuits, or the application of credible fault voltages on the devices output terminals, do not propagate back to the isolator's input terminals. The isolation devices provide confidence that, where protection signals are used by nonsafety systems, credible single failures in the nonsafety-related system do not degrade the performance of the safety-related system.

It is a design goal to minimize inadvertent reactor trips and engineered safety features actuations. Redundancy is provided for critical circuits which could malfunction and give an erroneous trip or engineered safety features initiation signal. The reactor trip circuit breaker arrangement illustrated in Figure 7.1-7 and described in subsection 7.1.2.5 is designed so that a single failure does not cause a reactor trip. The two-out-of-four actuation logic for reactor trip requires trip signals from two-out-of-four divisions. For engineered safety features initiation, the actuation logic for each component is performed redundantly within each engineered safety features actuation cabinet and is functionally treated as an "OR" function in the protection logic cabinets. This redundant logic, described in subsection 7.1.2.10, minimizes the probability of a random single failure causing inadvertent actuation. It also enables the safeguards actuation logic to meet single failure criterion during periodic testing. Dedicated switches which are used to initiate engineered safety features at the system level are connected to the engineered safety features actuation cabinets using two-pole, energize-to-actuate, ungrounded dc circuits. These circuits minimize inadvertent actuations caused by fire induced failures.

The design to reduce the likelihood of inadvertent trips or engineered safety features actuations does not negate the ability of the safety system to meet the single failure criterion, even when channels are bypassed for test or maintenance. Redundancy of equipment and the design bases applied to bypass capability demonstrate compliance to the single failure criterion.

7.1.4.2.3 Conformance to the Requirements for Quality Components and Modules (Paragraph 4.3 of IEEE 279-1971, GDC-1)

The quality of components and modules is consistent with use in a nuclear generating station protection system. Chapter 17 describes the AP600 quality assurance program.

7.1.4.2.4 Conformance to the Requirements for Equipment Qualification (Paragraph 4.4 of IEEE 279-1971, GDC-2, GDC-4, GDC-13, IEEE 323-1974, IEEE 344-1975, Regulatory Guide 1.89, Regulatory Guide 1.100, EICS-10)

Electrical equipment within the safety-related system is environmentally qualified to meet the conditions through which it must operate to mitigate the consequences of the accident. The environmental qualification program for Class 1E electrical equipment is discussed in Section 3.11. The seismic qualification program is discussed in Section 3.10.

7.1.4.2.5 Conformance to the Requirements to Maintain Channel Integrity (Paragraph 4.5 of IEEE 279-1971, GDC-2, GDC-3, GDC-4, Regulatory Guide 1.120)

The safety-related system instrumentation is designed to maintain its capability to initiate its protective functions during and following natural phenomena defined in Chapter 2 as credible to the plant, such as earthquakes, tornados, hurricanes, floods and winds. Functional capability of the system is maintained during events such as fires, flooding, explosions, missiles, electrical faults, and pipe whip as discussed in Chapter 3. The equipment is environmentally and seismically qualified as discussed in subsection 7.1.4.2.4.

Redundancy of equipment provides protective functions despite loss of one of the redundant divisions.

Potential causes of fire and missiles that might occur due to postulated faults within the safety system equipment are identified and addressed. Equipment is built to industry codes, standards, and practices aimed at maximizing reliability and safety. For example, wiring used within electrical equipment, and devices used to protect wiring from overcurrent (such as breakers, fuses, and current limiters), are sized and coordinated according to National Electric Code. Insulation used is flame retardant and meets National Electric Code, IEEE, and Underwriter's Laboratory guidelines applicable to the environment where the wiring is located. Electronics are housed in cabinets of metal construction. Isolation devices are incorporated into wiring leaving the protection cabinets to the other redundant protection cabinets or nonsafety-related areas. In addition, the fire ignition potential is limited by the low power level of the digital equipment. The independence of electrical equipment is verified as discussed in subsection 7.1.4.2.6.

7.1.4.2.6 Conformance to the Requirements to Maintain Channel Independence (Paragraph 4.6 of IEEE 279-1971, GDC-22, IEEE 384-1974, Regulatory Guide 1.75)

The flexibility of the protection and safety monitoring system enables physical separation of redundant divisions.

Where redundant equipment communicates, such as at the integrated protection cabinets, isolation devices are employed to preserve electrical independence of the divisions. These devices are described in subsection 7.1.2.11. They are also used to preserve the independence of safety equipment from nonsafety-related systems which may use protection signals.

Nonsafety-related wiring is separated from safety-related wiring as discussed in Chapter 8. Analyses, tests, or physical barriers are used to verify the adequacy of wire routing where separation distances are less than those suggested by regulatory guides or industry standards.

The physical separation criteria for protection system cabinets includes the applicable recommendations contained in Paragraph 6.6 of IEEE 384 (Reference 6). Specific criteria applied are the following:

- Internal separation criteria pertaining to separation between redundant Class 1E equipment according to Paragraph 6.2 of IEEE 384-81
- Non-Class 1E wiring criteria pertaining to separation between Class 1E wiring and non-Class 1E wiring according to Subparagraph 6.6.5 of IEEE 384-81
- Cable entrance criteria of redundant Class 1E cables according to Subparagraph 6.6.6 of IEEE 384-81

The application of these criteria to instrumentation cabinets is endorsed by Regulatory Guide 1.75.

Wiring for redundant divisions use physical separation, analyses, isolation, tests, or barriers to provide independence of the circuits.

7.1.4.2.7 Conformance to the Requirements Concerning Control and Protection System Interaction (Paragraph 4.7 of IEEE 279-1971, GDC-24)

Conformance to the Requirements on the Use of Isolation Devices

Signals from protection system equipment for control system use are transmitted through isolation devices. These devices are part of the protection system and meet Section 4 of IEEE 279-1971. The isolation devices are tested to confirm that credible failures at the output of the isolation device do not prevent the associated protection system channel from meeting the minimum performance requirements.

The isolation device is described in subsection 7.1.2.11. Credible failure tests include: physical damage; short circuits; open circuits; grounds; and the application of the maximum ac or dc potentials that may be present in any cabinet where the isolation device is located or in any wireway where its electrical or optical lines run.

Conformance to Requirements Concerning Control System Failures Interacting with the Protection System

The plant control system keeps the reactor operating away from safety limits. Should a control system fail and cause a parameter to approach its limit, the protection system trips the reactor as described in Section 7.2. The setpoints are chosen so that the design bases established for credible events are met. These design bases are discussed in subsection 7.1.4.1. The accident analyses in Chapter 15 do not assume a control system action to reduce the severity of an accident. Assumptions made on control systems are worst case assumptions - that their failure drives the parameters involved toward their worst direction for safety. The safety-related system setpoints account for these malfunctions.

As described in subsection 7.1.2.11, isolation devices are used to prevent credible faults in the control system from degrading the functional capability of the protection system.

Conformance to Requirements Concerning Protection System Failures Interacting with Control Systems

Certain information derived from protection channels is used to control the plant. This reduces the number of penetrations into critical pressure boundaries, such as into the reactor coolant loops, pressurizer and steam generators. It also helps reduce congestion and enhance separation.

A control system channel selection device is used so that malfunctioning protection channels do not send erroneous information to the control system. Protection system malfunctions in a channel do not cause a control system action that results in a protection function actuation using the remaining redundant channels monitoring that variable. Therefore, where protection signals are used for control, functional isolation is provided between the control and protection systems.

The selection device continuously monitors the redundant protection system channels, which send information to the control systems. The device provides the control system with signals considered valid.

As long as at least three redundant channels of information are available, an invalid signal is rejected by the selection device. This is done by comparing the redundant channels to one another. Any signal that deviates from the others by more than a reasonable amount is rejected, consistent with normal instrument channel drift and calibration tolerances. A detailed discussion of the signal selection algorithm used is contained in WCAP-13382 (Reference 3).

7.1.4.2.8 Conformance to Requirements Concerning the Derivation of System Inputs (Paragraph 4.8 of IEEE 279-1971)

To the extent feasible and practical, protection system inputs are derived from signals that are direct measures of the desired variables. These variables are listed in Section 7.2 for reactor trip and Section 7.3 for engineered safety features actuation.

The protection system calculates two variables where direct measurement is not feasible. These are the thermal overtemperature reactor trip and the thermal overpower reactor trip. These functions are described in subsection 7.2.1.1.3.

7.1.4.2.9 Conformance to the Requirements to Provide Capability for Sensor Checks (Paragraphs 4.9 of IEEE 279-1971, IEEE 338-1975, Regulatory Guide 1.118)

Means are provided for checking the operational availability of each protection system input sensor during reactor operation. These are accomplished by one of the following techniques:

- Perturbing the monitored variable
- Cross-checking between channels that have a known relationship to each other and that have read-outs available
- Introducing and varying a substitute input to the sensor of the same nature as the measured variable

7.1.4.2.10 Conformance to the Requirements to Provide Capability for Test and Calibration (Paragraph 4.10 of IEEE 279-1971, GDC-10, GDC-21, IEEE 338-1975, Regulatory Guide 1.22, Regulatory Guide 1.118, EICSB-5, EICSB-22)

Capability for testing and calibrating channels and devices used to derive the final system output signal from the various channel signals is provided.

Subsection 7.1.2.12 describes the built-in testing capabilities of the protection and safety monitoring system. These capabilities provide complete on-line overlapping testing of the protection and safety monitoring system from the inputs to the analog-to-digital converters, through the logic, to the actuation devices.

Where actuated equipment is not tested during reactor operation, it is established that:

- There is no practicable system design that permits operation of the equipment without adversely affecting the safety or operability of the plant.
- The probability that the protection system fails to initiate the operation of the actuated equipment is maintained acceptably low without testing the equipment during reactor operation.

- The equipment is routinely tested when the reactor is shutdown

When channels are bypassed for the purposes of testing, the bypass is automatically instated and removed by the built-in automatic tester. Bypass capability is discussed in subsection 7.1.2.10.

7.1.4.2.11 Conformance to Requirements on Channel Bypass or Removal from Operation (Paragraph 4.11 of IEEE 279-1971)

Provisions are made within the protection system for the application of bypasses, that is, blocks of certain protective functions during operational modes such as test and maintenance. The bypass system is designed so that applicable criteria are met, including the single failure criterion.

Channel Level Bypass Capability

A protection division takes inputs from one or more process sensors, performs compensation or other calculation, and terminates in one or more bistable functions where the process variable is compared against setpoints. The partial trip outputs from these comparisons are sent to the logic portion of the protection system. Here signals are combined with the partial trip status of the other channels to initiate a protective function, such as reactor trip.

When a channel is tested, the sensor input is removed and a test signal is injected in its place, and exercised over the range of that input sensor. This method of testing requires blocking the partial trips to preserve plant availability. The bypass system provides this blocking while at the same time assuring compliance to the single failure criterion. Each comparison function is provided with a bypass, which becomes an additional input to the logic downstream of the bistable functions. Interlocks are provided so that the gate, which admits the injected test signal to the channel, is not closed until that channel's functions have been bypassed.

The logic combines four bistable function outputs and their associated bypasses in a scheme that meets the single failure criterion, regardless of the number of bypasses applied. A description and evaluation of this logic is contained in WCAP-8897 (Reference 7). The effect of this logic scheme is to provide a two-out-of-four coincidence logic which reverts to a two-out-of-three when one bypass is applied. When two bypasses are applied, the logic reverts to a one-out-of-two logic. If three or more bypasses are simultaneously applied, the logic scheme provides the necessary output to initiate the protective action associated with the bypass, generally leading to a plant shutdown.

The bypass status, and the threshold function outputs, are transmitted between integrated protection cabinets by means of the isolated data links, described in subsection 7.1.2.9.

In addition to using the bypasses during channel test, they are used while maintenance is performed on the channel or if the channel sensor is failed and cannot be immediately repaired.

Generally there are four protection channels for each actuation function. Accident analyses or reliability studies assume that one of these channels is in the bypass mode at the time of the accident. The purpose of this assumption is to preclude potential limitations that might have otherwise been placed on the use of the bypass system.

Reactor Trip Breaker Bypass Capability

A reactor trip is actuated by opening pairs of reactor trip breakers, one pair is associated with each of four integrated protection cabinets. The breakers are arranged such that opening any two pairs of breakers de-energizes the control rod drive mechanisms, thus causing the reactor trip, as described in subsection 7.1.2.5. During maintenance and testing of the trip actuation logic, the trip signals to the undervoltage trip attachments of the reactor trip breakers are blocked. A description and evaluation of the logic are contained in WCAP-8897 (Reference 7). The logic automatically provides that no more than one pair (one division) of breakers can be bypassed at any one time. In the event that an attempt to bypass the breakers from one division occurs while another division is in the bypass mode, those breakers are tripped rather than bypassed. If a trip signal is generated by either of the two remaining divisions (one-out-of-two), the reactor trips. If more than two bypasses are actuated at a time, the reactor is tripped. The breaker bypass status is communicated between the integrated protection cabinets by the same system of isolated data links which carry the partial trip information. If a trip of two remaining breaker pairs occurs while one is in bypass, then that one is tripped as well.

Engineered Safety Features Bypass Capability

No engineered safety features system-level actuation logic bypasses (for test or maintenance) are provided. Instead, the actuation logic within the engineered safety features actuation cabinet is duplicated. Built-in test capabilities are discussed in subsection 7.1.2.12.

7.1.4.2.12 Conformance to Requirements on Operating Bypasses (Paragraph 4.12 of IEEE 279-1971)

In addition to the test and maintenance bypasses described in Section 7.1.4.2.11, several operating bypasses are provided. These bypasses automatically block certain protective actions that would otherwise prevent modes of operations such as start-up. The operating bypasses are automatically removed when the plant moves to an operating regime where the protective action is required if an accident occurred. These operating bypasses are discussed in subsections 7.2.1.1.11 and 7.3.1.3.

7.1.4.2.13 Conformance to Requirements to Provide Indication of Bypasses (Paragraph 4.13 of IEEE 279-1971, Regulatory Guide 1.47, EISCB-21)

Status indication for the channel level and the reactor trip breaker bypasses, described in subsection 7.1.4.2.11 are provided in the main control room. The display of the status information allows the operator to identify the specific functions that are bypassed, and also to determine if the logic has reverted to two-out-of-three or a one-out-of-two. In addition to

the status indication, an alarm is sounded in the main control room if more than one bypass has been applied to a given protection function, thus causing a one-out-of-two logic.

7.1.4.2.14 Conformance to Requirements Controlling Access to the Means for Bypassing (Paragraph 4.14 of IEEE 279-1971)

The bypasses described in subsection 7.1.4.2.11 are initiated in either of two ways, automatically via the automatic test system or manually via bypass switches. In either case, the operator has complete administrative control over bypass actuation. The automatic test sequence bypass is manually initiated and the manual bypass switches are located inside the integrated protection cabinets. The integrated protection cabinet doors are locked according to administrative procedures.

7.1.4.2.15 Conformance to the Requirements on the Use of Multiple Setpoints (Paragraph 4.15 of IEEE 279-1971, EICSB-12)

This subject is not applicable to the AP600 because setpoints are not made more restrictive as a function of operational mode.

7.1.4.2.16 Conformance to the Requirement for Completion of Protective Action Once it is Initiated (Paragraph 4.16 of IEEE 279-1971, Regulatory Guide 1.62)

Once initiated, protective functions at the system-level proceed to completion. The action of engineered safety features can be terminated on a component-by-component basis by deliberate operator intervention. Component-level manual reset controls permit the operator to take this action only after the system-level signal is reset. One of the reasons component reset is provided is to terminate safeguard functions if they are inadvertently actuated. Specific information for reactor trip is provided in subsection 7.2.2.2.7. Information on engineered safety features is provided in subsection 7.3.2.2.8.

7.1.4.2.17 Conformance to the Requirements for Manual Initiation of Protective Functions (Paragraph 4.17 of IEEE 279-1971, Regulatory Guide 1.62)

Manual initiation of protective functions at the system-level is available. Manual initiation circuits conform to the single-failure criterion as described in subsection 7.1.4.2.2. The specific manual actions are described in Section 7.2 for reactor trip, and in Section 7.3 for engineered safety features.

Manual initiation depends on the operation of the minimum of equipment. No single failure in either the automatic portion, manual portion, or shared portion prevents manual or automatic initiation of a protective function at the system level. This capability is achieved through the redundant structure of the protection and safety monitoring system.

7.1.4.2.18 Conformance to Requirements Governing Access to Setpoint Adjustments, Calibration, and Test Points (Paragraph 4.18 of IEEE 279-1971)

Access to setpoint adjustments, module calibrations, and test points is under administrative control. Cabinet doors are normally locked.

7.1.4.2.19 Conformance to the Requirements on Identification of Protective Actions (Paragraph 4.19 of IEEE 279-1971)

The initiation of a protective action is identified and indicated down to the channel-level. Except for post-accident monitoring information, this status information is not safety-related. As such it is transmitted to the main control room for indication and recording over isolated data links from the protection system.

7.1.4.2.20 Conformance to the Requirements for Information Read-Out (Paragraph 4.20 of IEEE 279-1971, Regulatory Guide 1.97)

Protection system status information is provided to the operator. Status information is of four types:

- Parameter values
- Logic status
- Equipment status
- Actuation device status

Safety-related displays are discussed in Section 7.5.

7.1.4.2.21 Conformance to the Requirement to Facilitate System Repair (Paragraph 4.21 of IEEE 279-1971)

The protection and safety monitoring system facilitates the recognition, location, replacement, repair and adjustment of malfunctioning components or modules. The built-in test capability described in subsection 7.1.2.12 provides a mechanism for periodically verifying the operability of modules in the protection and safety monitoring system, and of rapidly locating malfunctioning assemblies. Continuous on-line error checking also detects and locates failures. Channel bypass permits replacement of malfunctioning sensors or channel components, without jeopardizing plant availability, while still meeting the single-failure criterion.

7.1.4.2.22 Conformance to the Requirements for Identification of Redundant Safety System Equipment (Paragraph 4.22 of IEEE 279-1971)

Distinctive markings are applied to redundant divisions of the protection and safety monitoring system.

The color coded nameplates described below provide identification of equipment, associated with protective functions and their divisions associations.

Division	Color Coding
Division A	BROWN with WHITE lettering
Division B	GREEN with BLACK lettering
Division C	BLUE with WHITE lettering
Division D	YELLOW with BLACK lettering

Non-cabinet mounted protective equipment and components have an identification tag or nameplate. Small electrical components such as relays, have nameplates on the enclosure that houses them.

7.1.5 AP600 Protective Functions

Protective functions are those necessary to achieve the system responses assumed in the safety analyses, and those needed to shut down the plant safely. The protective functions are grouped into two classes, reactor trip and engineered safety features actuation. The software associated with these functions is considered a basic component as defined in Reference 10.

Reactor trip is discussed in Section 7.2. Engineered safety features actuation is discussed in Section 7.3.

7.1.6 Combined License Information

Combined License applicants referencing the AP600 certified design will provide a calculation of setpoints for protective functions consistent with the methodology presented in Reference 9.

7.1.7 References

1. IEEE 603-1991, "IEEE Criteria for Safety Systems for Nuclear Power Generator Stations."

2. IEEE 796-1983, "IEEE Microcomputer System Bus."

3. WCAP-13382 (P), WCAP-13391 (NP), "AP600 Instrumentation and Control Hardware Description," May 1992.

[*4. WCAP-13383, Revision 1 (NP), "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," June 1996.*]*

5. IEEE 279-1971, "IEEE Criteria for Protection Systems for Nuclear Power Generating Stations."

6. IEEE 384-1981, "IEEE Criteria for Independence or Class 1E Equipment and Circuits."

*NRC Staff approval is required prior to implementing a change in this material; see DCD Introduction Section 3.5.

7. WCAP-8897 (P), WCAP-8898 (NP), "Bypass Logic for the Westinghouse Integrated Protection System," Addendum 2, February 1994.

8. WCAP-14080 (P), WCAP-14081 (NP), "AP600 Instrumentation and Control Software Architecture and Operation Description," June 1994.

[*9. WCAP-14605 (P), WCAP-14606 (NP), "Westinghouse Setpoint Methodology for Protection Systems, AP600," April 1996*]*

10. 10 CFR 21, "Reporting of Defects and Noncompliance."

11. WCAP-11340 (P), "Noise, Fault, Surge, and Radio Frequency Interference Test Report," November 1986.

12. WCAP-13633 (P), WCAP-13634 (NP), "AP600 Instrumentation and Control Defense-in-Depth and Diverseity Report," April 1993.

*NRC Staff approval is required prior to implementing a change in this material; see DCD Introduction Section 3.5.

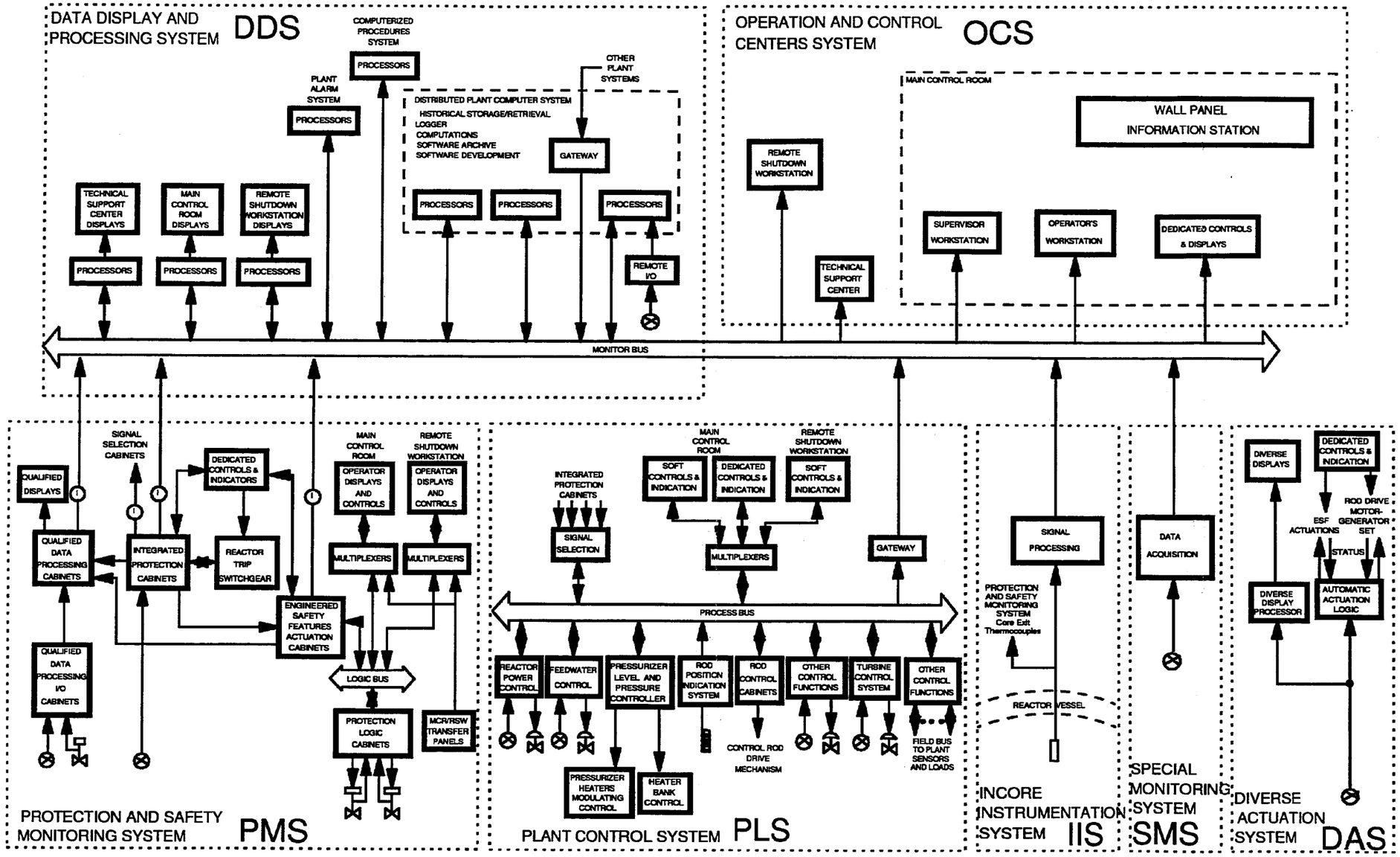

Figure 7.1-1

Instrumentation and Control Architecture

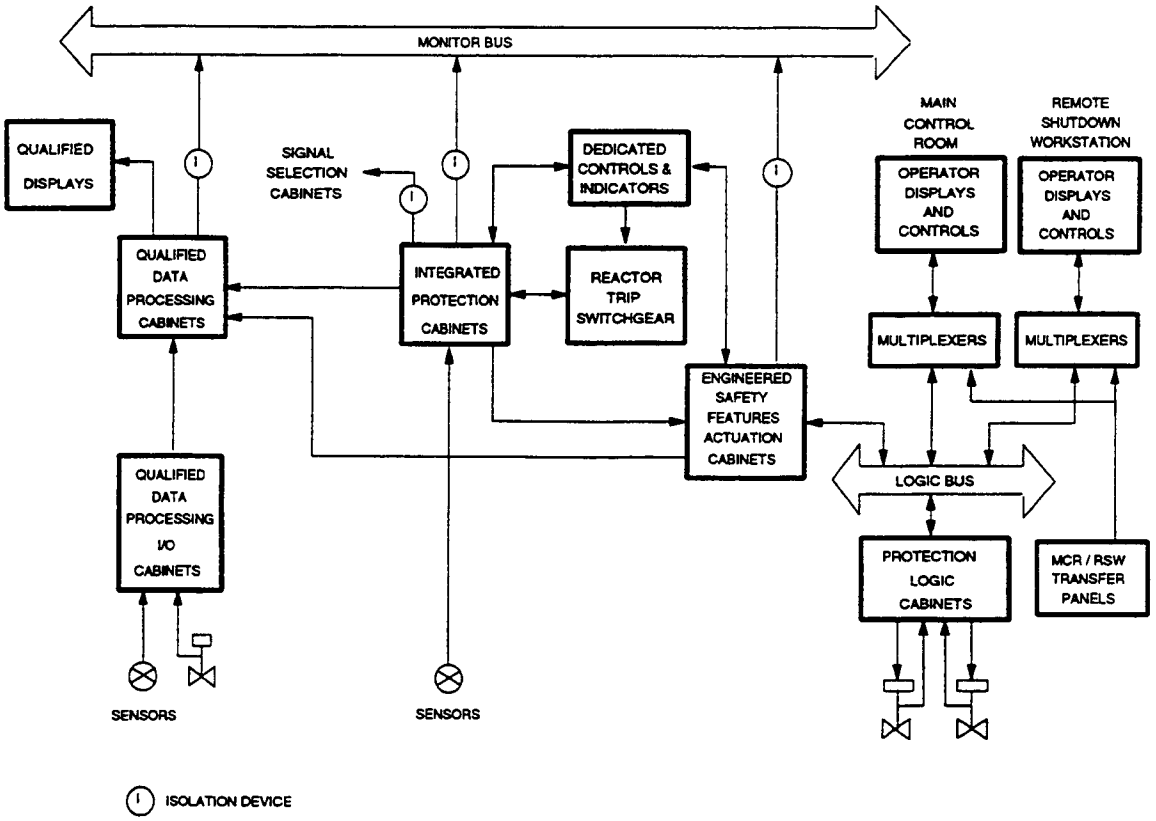

Figure 7.1-2

Protection and Safety Monitoring System

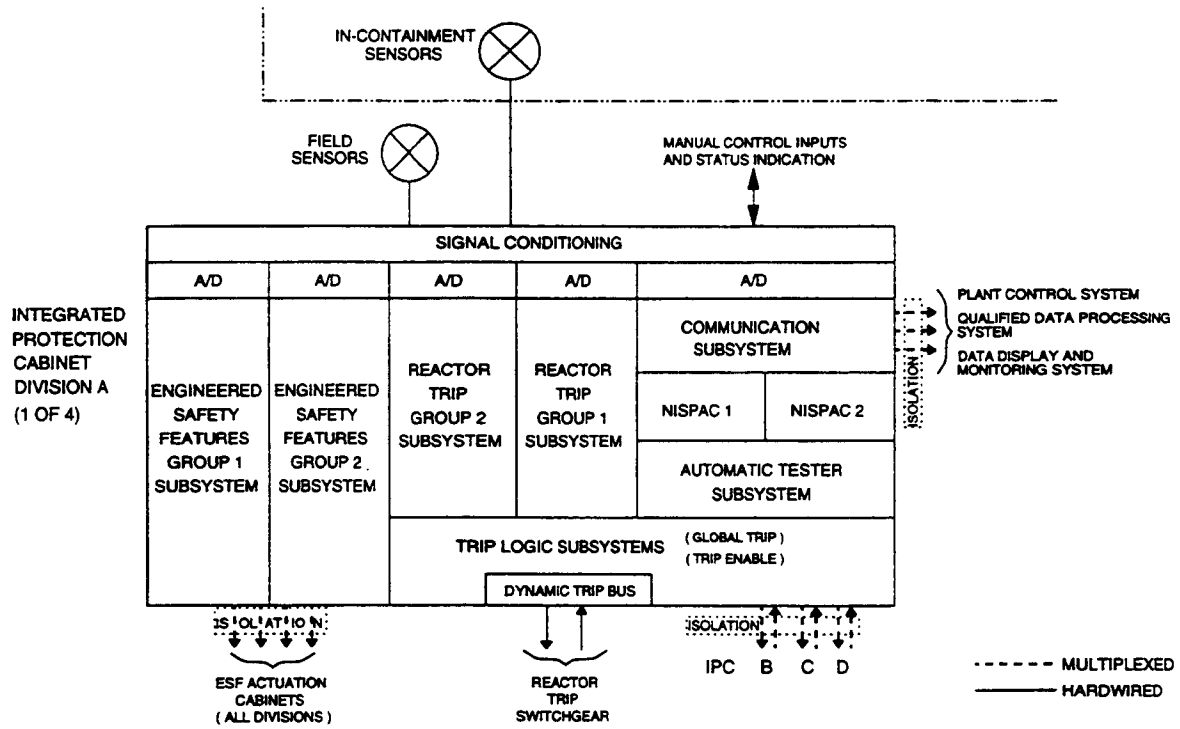

Figure 7.1-3

Integrated Protection Cabinet

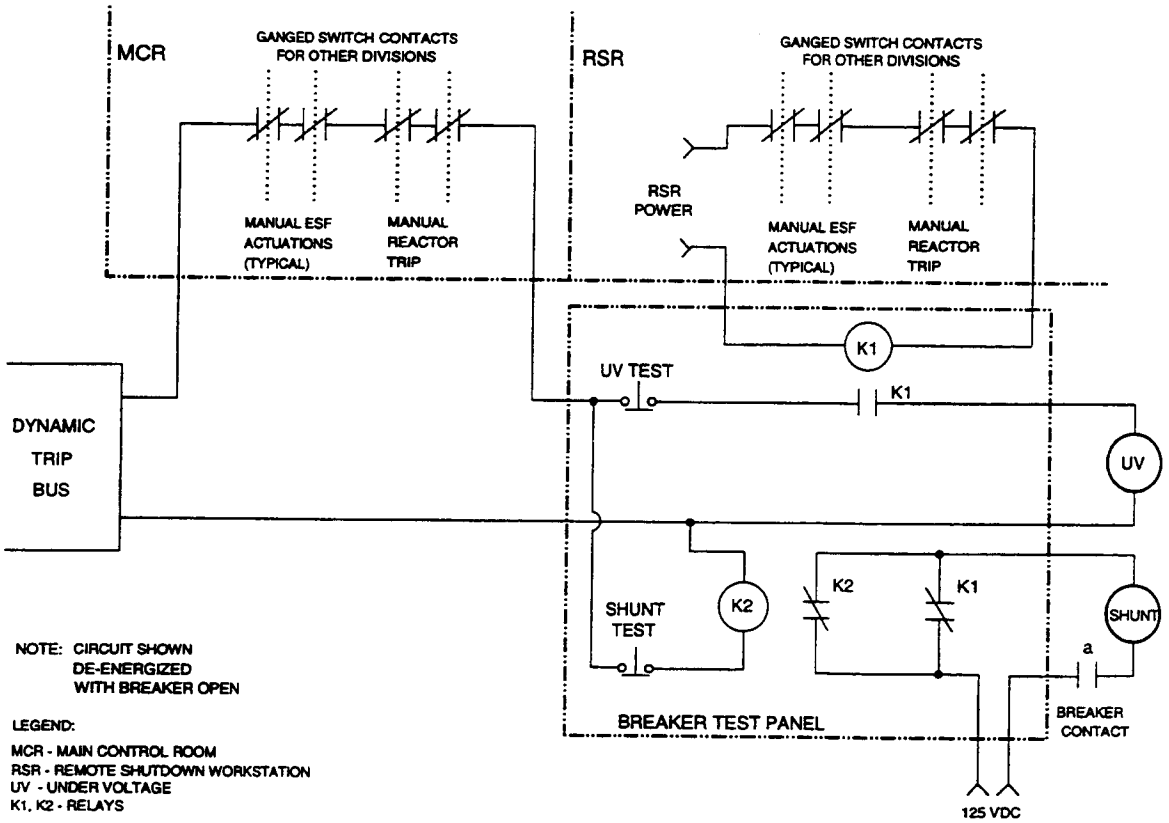

Figure 7.1-4

Reactor Trip Switchgear and Manual Trip Interface

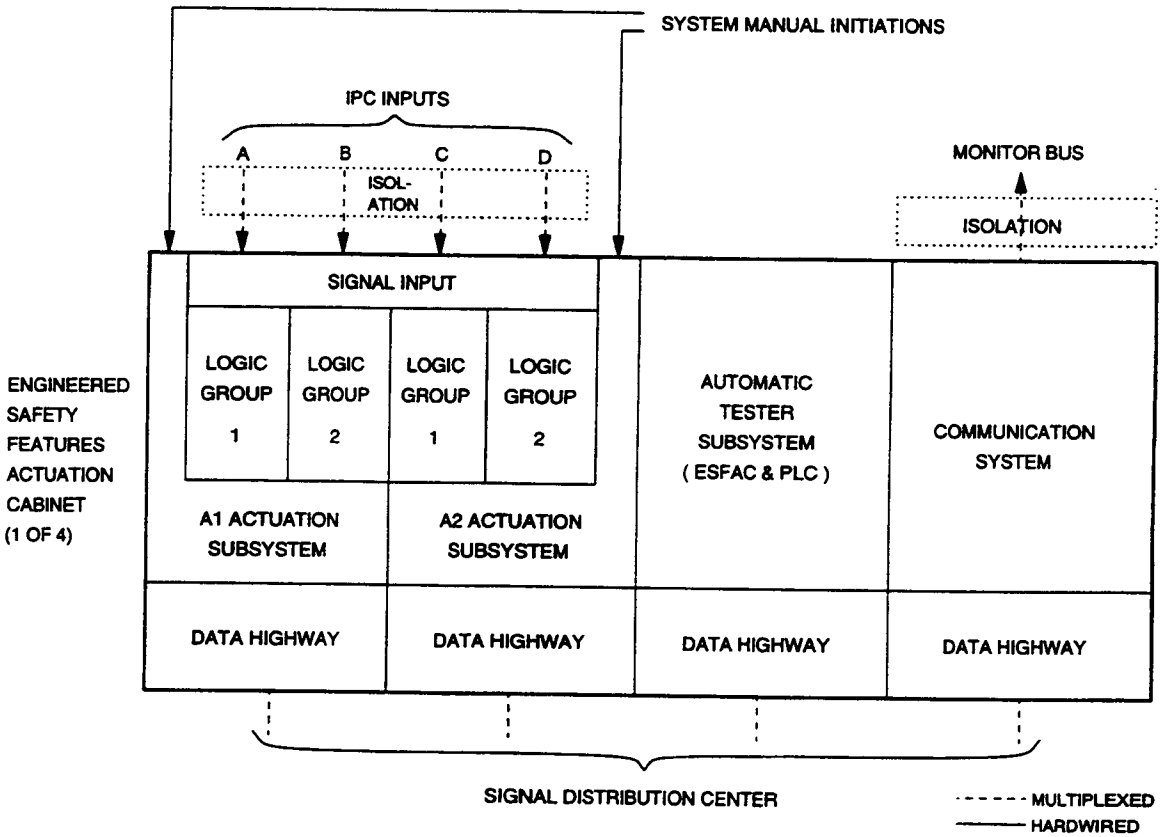

Figure 7.1-5

Engineering Safety Features Actuation Cabinet

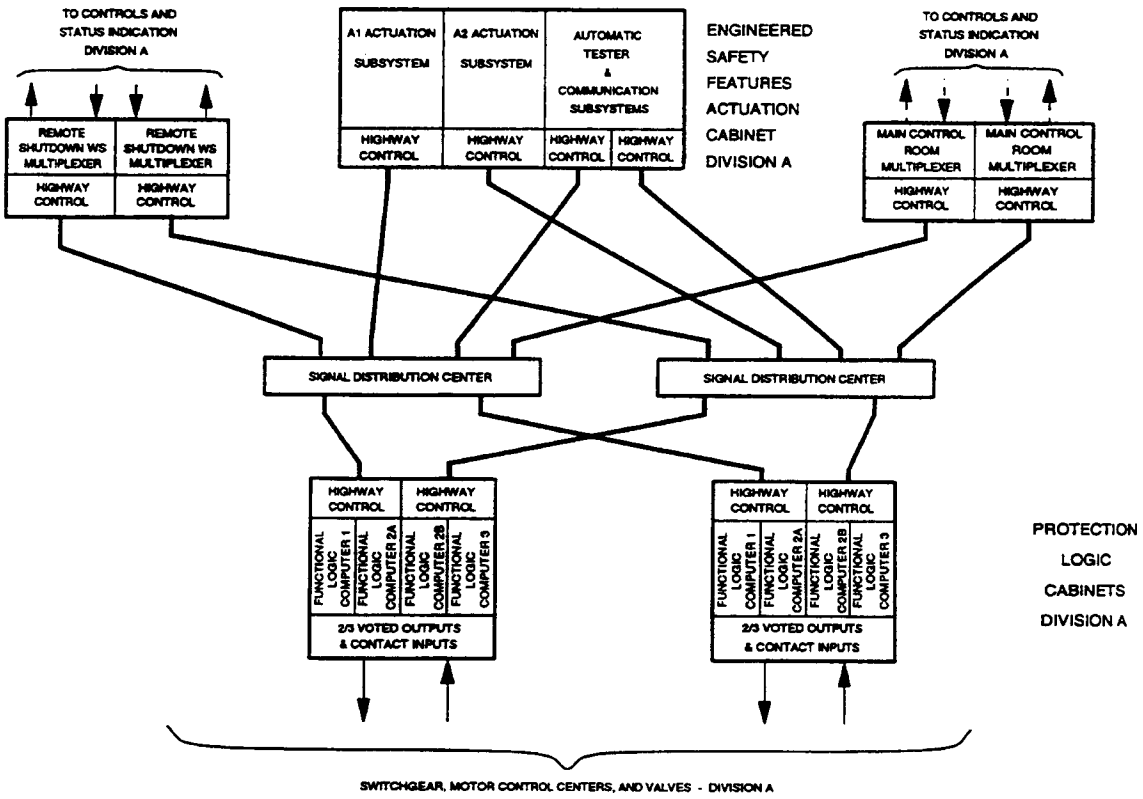

Figure 7.1-6

Protection Logic Communication Diagram

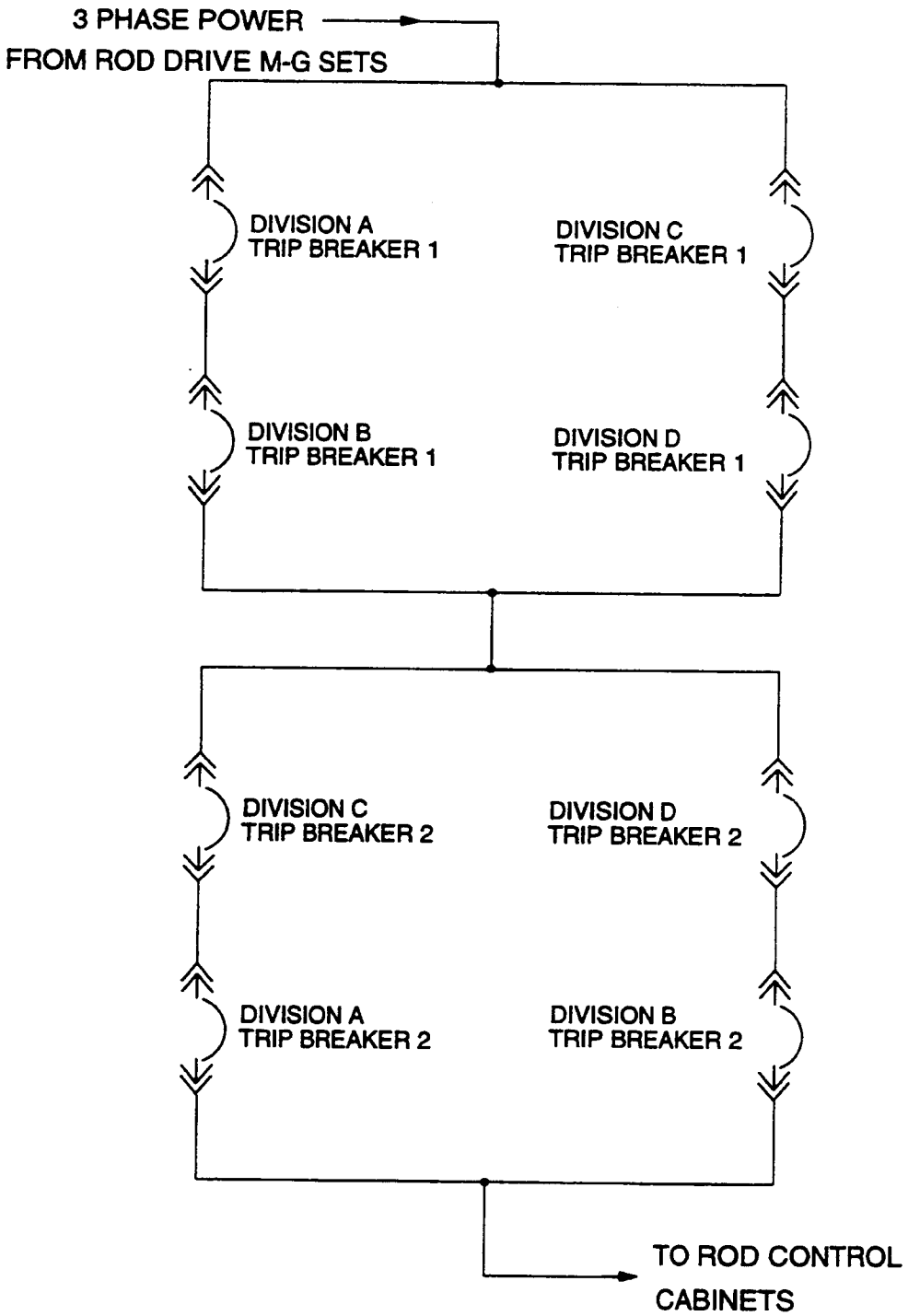

Figure 7.1-7

Reactor Trip Switchgear Configuration

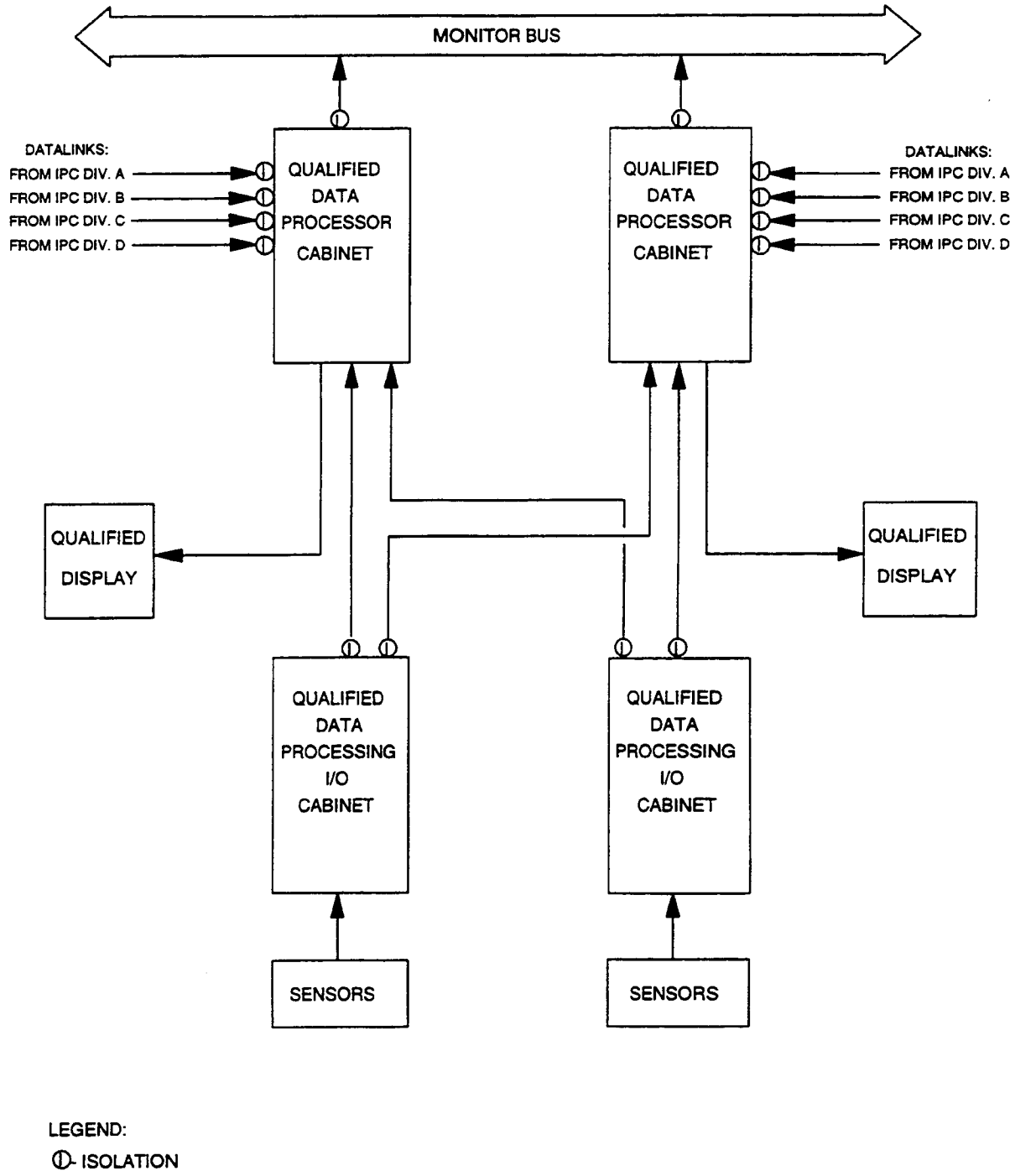

Figure 7.1-8

Qualified Data Processor

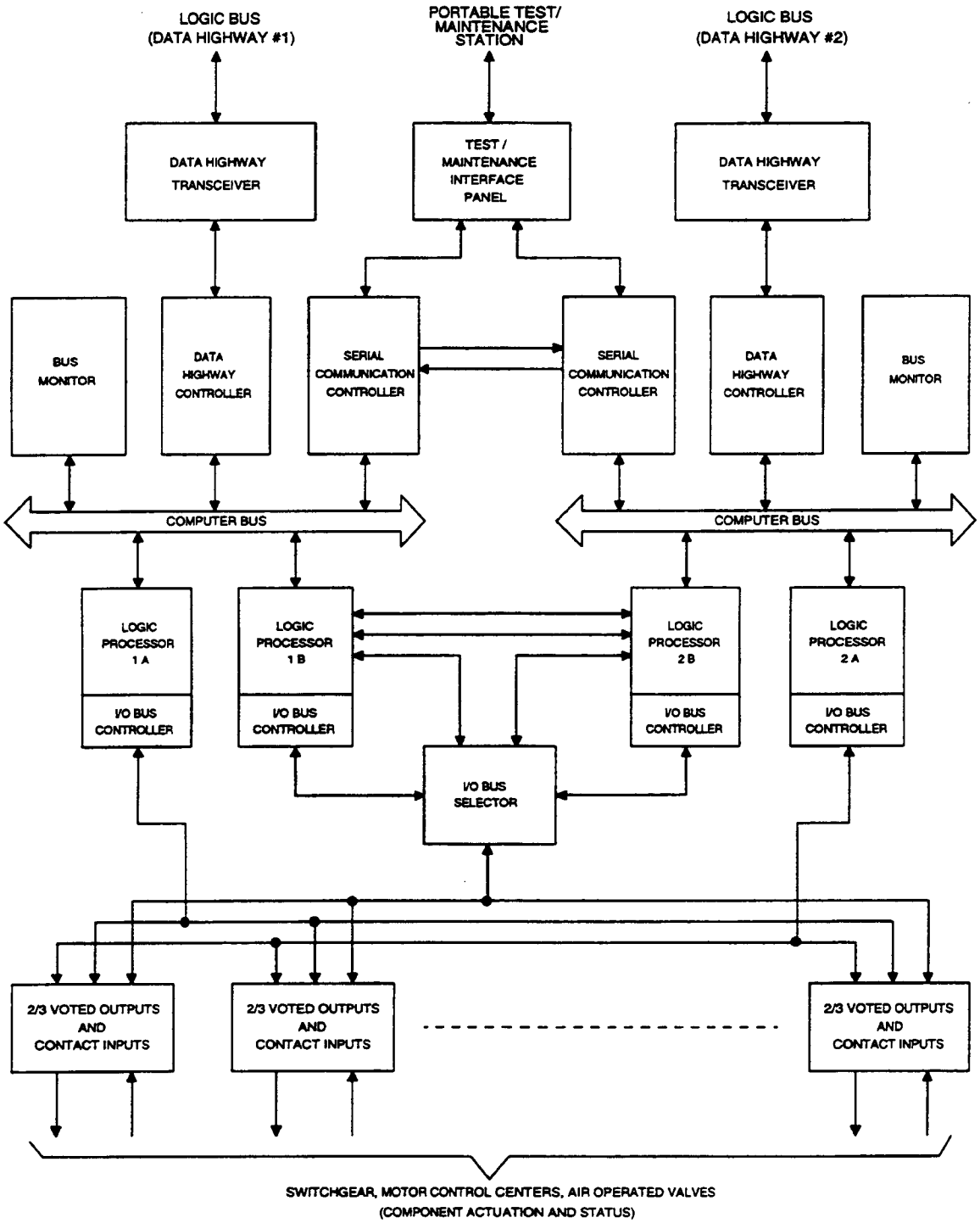

Figure 7.1-9

Protection Logic Cabinet Architecture

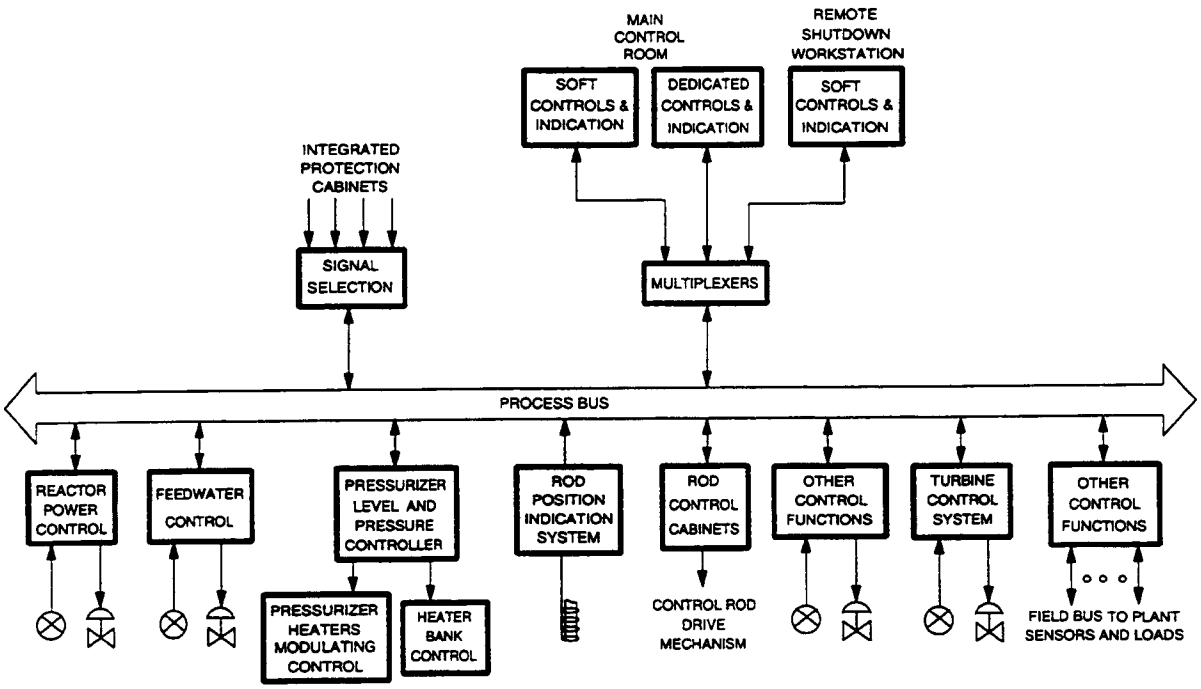

Figure 7.1-10

Plant Control System